

COURS

D'ALGÈBRE SUPÉRIEURE.

PARIS. — IMPRIMERIE DE MALLET-BACHELIER,
rue du Jardinet, nº 12.

COURS

D'ALGÈBRE SUPÉRIEURE

PROFESSÉ

A LA FACULTÉ DES SCIENCES DE PARIS;

PAR J.-A. SERRET,

Examinateur pour l'admission à l'École Polytechnique.



DEUXIÈME ÉDITION

REVUE ET AUGMENTÉE.

PARIS,

MALLET-BACHELIER, IMPRIMEUR-LIBRAIRE

DE L'ÉCOLE POLYTECHNIQUE ET DU BUREAU DES LONGITUDES,

QUAI DES AUGUSTINS, 55.

1854





AVERTISSEMENT.

Cet ouvrage ayant été favorablement accueilli par les Géomètres, je me décide à en faire paraître une deuxième édition. Je n'ai pas cru devoir changer la rédaction primitive, sauf en quelques points où des corrections de détail étaient nécessaires. La seule modification essentielle porte sur la vingt-cinquième leçon qui a été entièrement refondue et qui, jointe aux deux précédentes, offre maintenant une étude complète d'une partie de la théorie des nombres, indispensable dans l'analyse des équations algébriques.

Mais cette édition diffère surtout de la précédente par les Notes que j'ai ajoutées, et qui, toutes, se rattachent directement aux matières traitées dans l'ouvrage. On trouvera, dans ces Notes, un grand nombre de résultats nouveaux et des développements étendus sur quelques questions importantes qui ne sont qu'indiquées dans le texte.

En changeant l'objet de la vingt-cinquième leçon qui contenait des théorèmes élémentaires sur les nombres, et en la consacrant à l'exposition complète

et détaillée de la théorie des nouvelles quantités imaginaires considérées par Galois, je me suis proposé de faciliter l'intelligence d'une partie difficile des écrits de ce grand géomètre. Le beau Mémoire intitulé : *Sur les conditions de résolubilité des équations par radicaux,* ne laisse pas de présenter aussi quelques difficultés que j'aurais vivement désiré éclaircir en faisant connaître, dans l'une de mes Notes, le résultat de mes études sur cette théorie. Mais les considérations qui m'ont retenu lors de la première publication de cet ouvrage m'imposent encore aujourd'hui la même réserve.

AVERTISSEMENT

DE LA PREMIÈRE ÉDITION.

Cet ouvrage est le résumé des leçons que j'ai professées à la Sorbonne, dans la Chaire que la Faculté des Sciences m'a fait l'honneur de me confier cette année (1848).

Entièrement libre du choix des matières de mon Cours, j'ai développé la théorie de la résolution algébrique des équations, et les questions incidentes qui s'y rattachent. Je crois n'avoir omis aucun des faits principaux acquis à cette partie de la science.

La connaissance de l'Algèbre élémentaire, telle qu'elle est exposée dans l'excellent ouvrage de M. Lefébure de Fourcy, suffit pour l'intelligence des théories les plus importantes de ce livre. Toutefois, j'ai cru pouvoir faire usage du calcul différentiel et du calcul intégral, dans un petit nombre de passages.

Ces rédactions n'avaient pas été d'abord destinées

à l'impression : en les publiant, j'ai cédé au vœu exprimé par MM. les Professeurs qui m'ont fait l'honneur de suivre mon Cours. Je m'estimerai heureux si je contribue, par là, à propager l'étude d'une des parties les plus intéressantes et les moins connues de l'analyse.

I

TABLE DES MATIÈRES.

Pages.
Avertissement v
Avertissement de la première édition VII

PREMIÈRE LEÇON.

Introduction 1
Des fonctions symétriques 5
Formules de Newton pour calculer les sommes de puissances semblables des racines d'une équation 6
Usage de la division algébrique pour le même objet 9
Détermination des fonctions symétriques doubles, triples, etc., des racines d'une équation 11

DEUXIÈME LEÇON.

Méthode de Waring pour calculer une fonction symétrique rationnelle et entière des racines d'une équation 15
Méthode de M. Cauchy 25
Application de la méthode de M. Cauchy à un exemple 30

TROISIÈME LEÇON.

Formation de l'équation de laquelle dépend une fonction rationnelle et non symétrique des racines d'une équation donnée 33
Équation aux carrés des différences 35
Sur la forme des fonctions rationnelles d'une ou de plusieurs racines d'une équation 38
Méthode d'élimination fondée sur la théorie des fonctions symétriques 43
Théorème sur le degré de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations 44

QUATRIÈME LEÇON.

Méthode de M. Liouville pour la résolution de deux équations à deux inconnues 49
Extension au cas d'un nombre quelconque d'équations entre un même nombre d'inconnues 53
Méthode d'Abel pour déterminer la racine commune à deux équations. 57
Théorème de Lagrange sur les conditions nécessaires pour que deux équations aient plusieurs racines communes 62

CINQUIÈME LEÇON.

Pages.
Décomposition en fractions simples, d'une fraction rationnelle dont le dénominateur n'a pas de facteurs multiples... 68
Démonstration d'une formule d'analyse... 70
Méthode de M. Liouville pour décomposer une fraction rationnelle en fractions simples... 71
Cas des fractions rationnelles dont le dénominateur a des facteurs multiples... 74

SIXIÈME LEÇON.

Théorie générale de la décomposition des fractions rationnelles en fractions simples... 77
Théorèmes sur la possibilité de décomposer une fraction rationnelle. 78
Méthodes pour effectuer la décomposition d'une fraction rationnelle en fractions simples... 83

SEPTIÈME LEÇON.

Mode particulier de décomposition des fractions rationnelles dont le dénominateur a des facteurs linéaires imaginaires... 88
Conditions pour que l'intégrale d'une différentielle rationnelle soit algébrique... 94
Détermination du terme général d'une série récurrente... 97

HUITIÈME LEÇON.

Des fonctions symétriques et rationnelles des solutions communes à plusieurs équations... 102
Extension de la méthode d'élimination par les fonctions symétriques, au cas d'un nombre quelconque d'équations... 107
Théorème de Bezout sur le degré de l'équation finale... 109
Méthode de Tschirnaüs, pour faire disparaître autant de termes que l'on veut d'une équation... 113
Application aux équations du troisième et du quatrième degré... 116

NEUVIÈME LEÇON.

Développement d'une fonction algébrique implicite, en série ordonnée suivant les puissances décroissantes de sa variable... 118
Formation de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations à deux inconnues. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale... 122
Nouvelle démonstration d'une formule d'analyse... 127
Démonstration d'un théorème de géométrie... 128

DIXIÈME LEÇON.

Pages.
Développement en séries ordonnées suivant les puissances décroissantes de la variable de plusieurs fonctions algébriques définies par autant d'équations 133
Formation de l'équation finale qui résulte de l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale 136
Démonstration d'une formule de M. Jacobi 140
Extension du théorème de géométrie démontré dans la leçon précédente 142

ONZIÈME LEÇON.

Théorème sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme 145
Des fonctions semblables 149
Propriété des fonctions semblables des racines d'une équation ... 150
Examen des cas particuliers qui font exception 155
Méthode pour calculer une fonction des racines d'une équation, quand on connaît une autre fonction quelconque des racines 159

DOUZIÈME LEÇON.

Application de la théorie exposée dans la leçon précédente 163
Nouvelle démonstration d'un théorème établi dans cette leçon 165

TREIZIÈME LEÇON.

Propriétés des racines de l'équation binôme. Des racines primitives et de leur nombre 171
Digression sur la résolution numérique de l'équation à laquelle se ramène l'équation binôme, quand on lui applique la méthode d'abaissement des équations réciproques. Exposition de la méthode de M. Sturm pour la séparation des racines 183

QUATORZIÈME LEÇON.

Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction V_n 190
Expression du polynôme V_n 192
Expressions de $\cos na$ et de $\frac{\sin na}{\sin a}$ en fonction de $\cos a$ 194

Pages.
Expression du polynôme U_n. 195
Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction U_n. 196
Nouvelle manière de démontrer la réalité des racines des équations $V_n = 0$, $U_n = 0$ 198

QUINZIÈME LEÇON.

Résolution de l'équation générale du troisième degré 201
Méthode de Hudde 201
Méthode de Lagrange 209
Comparaison des deux méthodes précédentes 214
Méthode de Tschirnaüs 216
Méthode d'Euler 217

SEIZIÈME LEÇON.

Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième et des quantités connues 218
Étude d'une classe étendue d'équations numériques du troisième degré, qui possèdent une propriété remarquable 223

DIX-SEPTIÈME LEÇON.

Résolution de l'équation générale du quatrième degré 233
Méthode de Louis Ferrari 233
Étude de la résolvante 235
Méthode de Lagrange 237
Méthode de Descartes 242
Méthodes de Tschirnaüs et d'Euler 243

DIX-HUITIÈME LEÇON.

Sur la résolution algébrique des équations 244
Des équations de degré premier 246
Des équations de degré non premier 255

DIX-NEUVIÈME LEÇON.

Sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme 263
Des substitutions circulaires 266
Théorème de M. Cauchy 269
Forme générale des fonctions qui ont deux valeurs 275

VINGTIÈME LEÇON.

Pages.

Théorème de M. Bertrand sur le nombre des valeurs que peut prendre une fonction de *n* lettres ... 277
Forme générale des fonctions de *n* lettres qui ont *n* valeurs distinctes. 282
Examen des cas particuliers qui échappent à la démonstration précédente ... 283

VINGT ET UNIÈME LEÇON.

Des fonctions algébriques... 289
Des fonctions entières... 290
Des fonctions rationnelles ... 291
Classification des fonctions algébriques non rationnelles ... 291
Forme générale des fonctions algébriques... 294

VINGT-DEUXIÈME LEÇON.

Propriétés des fonctions algébriques qui satisfont à une équation donnée... 299
Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième... 304

VINGT-TROISIÈME LEÇON.

Des nombres congrus ou équivalents ... 310
Théorème de Fermat... 314
Théorème de Wilson... 315
Des congruences en général... 316
Limite du nombre des racines d'une congruence suivant un module premier... 318
Détermination du nombre de racines d'une congruence... 321
Nouvelle démonstration du théorème de Wilson... 324

VINGT-QUATRIÈME LEÇON.

Propriétés des racines des congruences binômes de module premier. 325
De l'existence des racines primitives... 328
Du nombre des racines primitives... 331
Recherche des racines primitives d'un nombre premier ... 332
Table des racines primitives des nombres premiers inférieurs à 100. 340
Propriété des racines de l'équation $x^m - 1 = 0$, dont le degré *m* est un nombre premier... 341

VINGT-CINQUIÈME LEÇON.

Pages.

Des congruences irréductibles suivant un module premier 343

Des nouvelles quantités imaginaires qui naissent de la théorie des nombres 348

Des racines d'une congruence irréductible 352

De la congruence $x^{p^\nu} - x \equiv 0 \pmod{p}$ 356

Propriété des racines d'une congruence irréductible 361

Des racines primitives 362

Recherche de toutes les racines d'une congruence quelconque 366

Application de la théorie à un exemple 367

VINGT-SIXIÈME LEÇON.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre 372

VINGT-SEPTIÈME LEÇON.

Résolution algébrique des équations dont toutes les racines peuvent être représentées par $x, \theta x, \theta^2 x, \ldots, \theta^{\mu-1} x$, θx étant une fonction rationnelle de x et de quantités connues, telle que $\theta^{\mu} x = x$. 385

Cas où les quantités connues de f et de θ sont réelles 390

Première méthode particulière relative aux équations dont le degré est un nombre composé 392

Deuxième méthode 397

VINGT-HUITIÈME LEÇON.

Résolution algébrique des équations dont dépend la division de la circonférence du cercle en un nombre premier de parties égales 400

Division de la circonférence en dix-sept parties égales 406

Construction géométrique 410

VINGT-NEUVIÈME LEÇON.

Formule de Lagrange pour le développement de certaines fonctions implicites 415

Développement d'une racine de l'équation $z = x + tz^m$ 422

Autre application de la formule de Lagrange 423

TRENTIÈME LEÇON.

Pages.

Solution d'un problème d'analyse indéterminée relatif à la représentation géométrique des fonctions elliptiques.................. 424

NOTE I.

Sur la détermination des sommes de puissances semblables des racines d'une équation.................................. 431

NOTE II.

Sur l'expression d'une fonction symétrique d'ordre quelconque des racines d'une équation, en fonction des sommes de puissances semblables des racines.................................... 442

NOTE III.

Sur la détermination du dernier terme de l'équation aux carrés des différences.. 452

NOTE IV.

Sur la décomposition des fractions rationnelles en fractions simples. 457

NOTE V.

Sur une application de la méthode de Tschirnaüs............... 462

NOTE VI.

Sur l'élimination d'une inconnue entre deux équations............ 465

NOTE VII.

Sur une classe d'équations qui possèdent une propriété remarquable... 476

NOTE VIII.

Sur le nombre des valeurs que peut prendre une fonction quand on on y permute les lettres qu'elle renferme....... 493

NOTE IX.

Pages.

Sur l'équation $\frac{x^p - 1}{x - 1} = 0$, où p désigne un nombre premier..... 516

NOTE X.

Sur une propriété remarquable de la fonction $\frac{x^p - 1}{x - 1}$, où p désigne un nombre premier..... 522

NOTE XI.

Sur la loi de réciprocité qui existe entre deux nombres premiers quelconques..... 533

NOTE XII.

Sur la résolutien algébrique de l'équation du neuvième degré à laquelle eondult la recherche des points d'inflexlen des courbes du troisième degré..... 538

NOTE XIII.

Sur les éqnations réselubles algébriquement..... 560

NOTE XIV.

Sur l'évalnation approchée du produit 1.2.3... x quand x est un grand nembre..... 576

NOTE XV.

Sur la totalité des nombres premiers compris entre deux limites données et sur le postulatum admis dans la vingtième leçon..... 587

Une planche.

FIN DE LA TABLE DES MATIÈRES.

COURS
D'ALGÈBRE SUPÉRIEURE.

PREMIÈRE LEÇON.

Introduction. — Des fonctions symétriques. — Formules de Newton pour calculer les sommes de puissances semblables des racines d'une équation. — Usage de la division algébrique pour le même objet. — Détermination des fonctions symétriques doubles, triples, etc., des racines d'une équation.

Introduction.

L'Algèbre est, à proprement parler, l'*Analyse des équations;* les diverses théories partielles qu'elle comprend se rattachent toutes, plus ou moins, à cet objet principal. A ce point de vue, l'Algèbre peut se diviser en trois parties bien distinctes :

1°. *La théorie générale des équations*, c'est-à-dire l'ensemble des propriétés qui sont communes à toutes les équations;

2°. *La résolution des équations numériques,* c'est-à-dire la détermination des valeurs exactes ou approchées des racines d'une équation dont les coefficients sont donnés en nombres;

3°. *La résolution algébrique des équations,* c'est-à-dire la détermination d'une expression composée avec les coefficients d'une équation donnée, et qui, substituée à l'inconnue, satisfasse identiquement à cette équation, soit que les coefficients de l'équation proposée soient *nu-*

mériquement donnés, soit qu'étant simplement considérés comme connus, ils restent indéterminés et représentés par des lettres.

Je me propose, dans ce Cours, d'exposer spécialement les recherches que les géomètres ont entreprises jusqu'à nos jours *sur la résolution algébrique des équations*, en admettant comme connues les *propriétés générales des équations*, et la plupart des principes sur lesquels repose leur résolution numérique. Je me réserve, toutefois, de revenir sur quelques points principaux de ces deux théories, qui se rattachent à l'objet de nos investigations.

Sans prétendre faire ici l'histoire complète de l'Algèbre, je crois devoir, dès à présent, donner un aperçu des principaux résultats acquis à cette partie de la science que nous allons étudier.

Il serait difficile de dire à qui nous devons la résolution des équations du second degré: elle se trouve dans le livre de Diophante, et, comme le fait remarquer Lagrange dans son *Traité de la Résolution des équations numériques*, elle ressort naturellement de quelques propositions d'Euclide. Luc Paciolo, qui publia en 1494, à Venise, le premier livre d'Algèbre paru en Europe, ne fait aucune mention de Diophante, et laisse supposer que les algébristes italiens avaient appris des Arabes ce qu'ils savaient d'algèbre, c'est-à-dire la résolution des équations du premier et du second degré.

La résolution des équations du troisième degré est due à deux géomètres italiens du XVI[e] siècle, Scipion Ferrei et Tartaglia; mais on ignore par quel chemin ils y ont été conduits, et la formule qui représente les trois racines de l'équation du troisième degré est communément appelée la *formule de Cardan*.

C'est aussi à un géomètre italien, Louis Ferrari, disciple de Cardan, que l'on doit la résolution de l'équation



du quatrième degré. Depuis, plusieurs méthodes, que nous indiquerons successivement, ont été proposées pour la résolution des équations du troisième et du quatrième degré; mais Lagrange a montré, dans un excellent Mémoire inséré parmi ceux de l'Académie de Berlin, pour 1770 et 1771, que ces méthodes, différentes en apparence, reviennent toutes, au fond, à faire dépendre la résolution de l'équation proposée, de celle d'une seconde équation qu'il appelle *résolvante*, et dont la racine est composée linéairement avec celles de la proposée et les puissances d'une racine de l'unité du même degré. En cherchant à généraliser cette méthode, à l'étendre aux équations de tous les degrés, ce grand géomètre a montré qu'au delà du quatrième degré, l'équation résolvante était d'un degré supérieur à celui de la proposée, et ne paraissait pas, en général, susceptible d'abaissement. Il a enfin fait voir clairement, par cette analyse, à quelle circonstance est due la résolution générale des équations des quatre premiers degrés, circonstance qui ne se présente plus au delà du quatrième degré.

Toutefois, la méthode de Lagrange peut être employée utilement dans la résolution des équations binômes, ou, ce qui revient au même, des équations dont dépend la division de la circonférence du cercle en parties égales. La résolution de ces équations avait été effectuée antérieurement et pour la première fois par M. Gauss, à l'aide d'une méthode ingénieuse fondée sur les relations qui existent entre les diverses racines de l'équation binôme, et sur la considération des *racines primitives* des nombres premiers.

Abel, généralisant les résultats obtenus par M. Gauss, a montré ensuite que si deux racines d'une équation *irréductible* sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre, l'équation est

soluble par radicaux, si son degré est un nombre premier, et que, dans le cas contraire, sa résolution dépend de celle d'équations de degrés moindres que le sien. C'est là un des plus beaux résultats dont l'Algèbre se soit enrichie de nos jours. Abel a fait, dans son Mémoire, l'application de sa méthode aux équations binômes, et a apporté quelques simplifications à l'analyse de M. Gauss.

Voici donc une classe assez étendue d'équations dont les racines peuvent être exprimées par radicaux; mais ces équations, étudiées par Abel, sont-elles les seules qui possèdent cette propriété? Dans quel cas, en un mot, une équation peut-elle être résolue algébriquement? Cette question difficile a été résolue complétement, au moins pour les équations irréductibles de degré premier, par Évariste Gallois, ancien élève de l'École Normale, et l'un des géomètres les plus profonds que la France ait produits. Dans un Mémoire présenté à l'Académie des Sciences en 1831, et publié en 1846 par les soins de M. Liouville, Gallois a, en effet, démontré ce beau théorème: *Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que, deux quelconques des racines étant données, les autres s'en déduisent rationnellement.*

Enfin, quant aux équations dont les racines sont des quantités quelconques n'ayant entre elles aucune dépendance, c'est-à-dire dont les coefficients restent indéterminés, leur résolution générale est impossible au delà du quatrième degré. Cette proposition importante, énoncée par Ruffini, a été mise hors de doute par les travaux plus récents d'Abel.

Tels sont les travaux les plus importants qui aient été entrepris sur la résolution algébrique des équations, et dont j'ai cru devoir faire ici l'indication succincte.

Nous commencerons ce Cours par l'exposition d'une

théorie fort simple, des principes de laquelle nous ferons un usage fréquent, et que, pour cette raison, je crois devoir rappeler avec quelques détails; je veux parler de la théorie des fonctions symétriques.

Des fonctions symétriques.

Une fonction de plusieurs quantités est dite *symétrique*, lorsque sa valeur n'est pas changée par les diverses permutations des quantités qu'elle renferme; nous ne nous occuperons ici que des fonctions symétriques *rationnelles*.

Les coefficients d'une équation algébrique sont des fonctions symétriques des racines de cette équation; ce sont même les fonctions symétriques les plus simples, puisque chaque racine n'y entre qu'au premier degré. S'il s'agit, en effet, de l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

et que a, b, c,..., k, l désignent les m racines, on sait que l'on a

$$\begin{aligned} a + b + c + \ldots + k + l &= -p_1, \\ ab + ac + \ldots + kl &= p_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ abc\ldots kl &= \pm p_m. \end{aligned}$$

Nous allons montrer comment on peut trouver l'expression d'une fonction symétrique et rationnelle quelconque des racines d'une équation, et cette recherche nous conduira à ce théorème important :

Toute fonction rationnelle et symétrique des racines d'une équation peut s'exprimer rationnellement par les coefficients de cette équation.

Examinons d'abord à quoi peut se réduire la recherche de la fonction symétrique et rationnelle la plus générale

possible. Toute fonction rationnelle non entière est le quotient de deux fonctions entières, en sorte qu'il n'y a lieu de s'occuper que des fonctions symétriques entières. En outre, toute fonction symétrique entière non homogène est la somme de deux ou plusieurs fonctions symétriques homogènes; tout est donc ramené à établir des règles pour calculer les fonctions symétriques rationnelles entières et homogènes; enfin, une pareille fonction symétrique entière et homogène peut contenir des termes où les exposants des lettres, tout en ayant la même somme, ne soient pas égaux chacun à chacun : dans ce cas, la fonction est la somme de deux ou d'un plus grand nombre de fonctions symétriques de même degré, mais différentes, et que nous calculerons séparément. De tout cela, il résulte que nous pourrons nous borner à la détermination des fonctions symétriques rationnelles, entières et homogènes, telles que les exposants des lettres soient les mêmes dans deux termes quelconques. Toute fonction de cette espèce sera déterminée si l'on connaît un seul de ses termes, ainsi que toutes les lettres qui entrent dans sa composition. Cela posé, nous appellerons *fonction symétrique simple ou du premier ordre,* une fonction symétrique rationnelle, entière et homogène, dont chaque terme ne contient qu'une seule lettre; *fonction symétrique double ou du deuxième ordre,* celle dont chaque terme renferme deux lettres, et ainsi de suite.

Formules de Newton pour calculer les sommes de puissances semblables des racines d'une équation.

Soit l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

que nous représenterons aussi, pour abréger, par

$$X = 0,$$

et dont nous désignerons par $a, b, c, \ldots, k, l$ les m racines. Soit, en outre, X' le polynôme dérivé de X; on aura

$$X' = mx^{m-1} + (m-1)p_1 x^{m-2} + \ldots + 2p_{m-2}x + p_{m-1}.$$

On a aussi, par un théorème connu,

$$X' = \frac{X}{x-a} + \frac{X}{x-b} + \ldots + \frac{X}{x-l};$$

et l'on trouve, par la division,

$$\frac{X}{x-a} = \begin{array}{r|r|r|rr}
x^{m-1}+a & x^{m-2}+a^2 & x^{m-3}+a^3 & x^{m-4}+\ldots & +a^{m-1} \\
+p_1 & +p_1 a & +p_1 a^2 & & +p_1 a^{m-2} \\
 & +p_2 & +p_2 a & & +p_2 a^{m-3} \\
 & & +p_3 & & +\ldots\ldots \\
 & & & & +\ \ldots\ldots \\
 & & & & +p_{m-2}a \\
 & & & & +p_{m-1}.
\end{array}$$

Si, dans cette équation, on remplace successivement a par chacune des autres racines, et qu'on fasse généralement

$$s_n = a^n + b^n + c^n + \ldots + k^n + l^n,$$

on aura, en ajoutant tous les résultats, la valeur suivante de X',

$$X' = \begin{array}{r|r|r|rr}
mx^{m-1}+s_1 & x^{m-2}+s_2 & x^{m-3}+s_3 & x^{m-4}+\ldots & +s_{m-1} \\
+mp_1 & +p_1 s_1 & +p_1 s_2 & & +p_1 s_{m-2} \\
 & +mp_2 & +p_2 s_1 & & +p_2 s_{m-3} \\
 & & +mp_3 & & +\ldots\ldots \\
 & & & & \ldots\ldots \\
 & & & & \ldots\ldots \\
 & & & & +p_{m-2}s_1 \\
 & & & & +mp_{m-1}.
\end{array}$$

La comparaison de cette valeur de X' avec celle écrite

plus haut, fournit les relations suivantes :

$$(1)\left\{\begin{array}{l} s_1+p_1=0,\\ s_2+p_1s_1+2p_2=0,\\ s_3+p_1s_2+p_2s_1+3p_3=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ s_{m-1}+p_1s_{m-2}+p_2s_{m-3}+\ldots+p_{m-2}s_1+(m-1)p_{m-1}=0. \end{array}\right.$$

La première de ces équations fait connaître s_1 ou la somme des racines, la seconde fait connaître s_2 ou la somme de leurs carrés, et ainsi de suite, jusqu'à la dernière qui fait connaître s_{m-1}.

On trouve de cette manière

$$\begin{array}{l} s_1=-p_1,\\ s_2=p_1^2-2p_2,\\ s_3=-p_1^3+3p_1p_2-3p_3,\\ s_4=p_1^4-4p_1^2p_2+4p_1p_3+2p_2^2-4p_4,\\ s_5=-p_1^5+5p_1^3p_2-5p_1^2p_3-5(p_2^2-p_4)p_1+5(p_2p_3-p_5),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Voici maintenant comment on peut former les sommes de puissances semblables, dont le degré surpasse $m-1$, et celles dont le degré est négatif. Soit n un nombre entier positif, nul ou négatif, et multiplions l'équation proposée par x^n ; elle deviendra

$$x^{m+n}+p_1x^{m+n-1}+p_2x^{m+n-2}+\ldots+p_{m-1}x^{n+1}+p_mx^n=0.$$

Remplaçons successivement x par chacune des racines a, b, c, etc., et ajoutons tous les résultats ; on aura

$$s_{m+n}+p_1s_{m+n-1}+p_2s_{m+n-2}+\ldots+p_{m-1}s_{n+1}+p_ms_n=0;$$

en donnant à n les valeurs 0, 1, 2, etc., et observant que

$s_0 = m$, on obtiendra les relations suivantes :

$$(2)\quad \begin{cases} s_m \quad + p_1 s_{m-1} + p_2 s_{m-2} + \ldots + p_{m-1} s_1 + m p_m = 0, \\ s_{m+1} + p_1 s_m \quad + p_2 s_{m-1} + \ldots + p_{m-1} s_2 + p_m s_1 = 0, \\ s_{m+2} + p_1 s_{m+1} + p_2 s_m \quad + \ldots + p_{m-1} s_3 + p_m s_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

Les sommes $s_1, s_2, \ldots, s_{m-1}$ étant connues par les équations (1), la première des équations (2) déterminera s_m, la seconde s_{m+1}, et ainsi de suite. Il importe de remarquer que les valeurs des sommes s_1, s_2, etc., ne contiendront, dans leur expression, aucun dénominateur, et que si les coefficients p_1, p_2, etc., sont des nombres entiers, les sommes s_1, s_2, etc., seront aussi des nombres entiers.

Réciproquement, si l'on connaît m sommes de puissances semblables, par exemple $s_1, s_2, \ldots, s_m$, on pourra déterminer les coefficients p_1, p_2, etc., à l'aide des équations (1) et (2), qui ont été données, pour la première fois, par Newton.

On pourra calculer aussi les sommes de puissances semblables des racines à exposants négatifs, en donnant au nombre n, que nous avons introduit, les valeurs successives -1, -2, -3, etc.; mais à l'égard de ces sommes de puissances négatives, le moyen le plus aisé de les trouver, consiste à changer x en $\frac{1}{x}$ dans l'équation proposée, et à calculer ensuite les sommes de puissances semblables à exposants positifs, des racines de l'équation transformée.

Usage de la division algébrique pour le même objet.

On peut employer, pour calculer les sommes des puissances semblables des racines d'une équation, une autre

méthode qui n'exige qu'une simple division algébrique. Soit toujours

$$X = 0$$

une équation ayant pour racines $a, b, c, \ldots, k, l$. Si X' représente la dérivée de X, on a, comme précédemment,

$$\frac{X'}{X} = \frac{1}{x-a} + \frac{1}{x-b} + \cdots + \frac{1}{x-l}.$$

En développant $\frac{1}{x-a}$ suivant les puissances négatives et décroissantes de x, on trouve

$$\frac{1}{x-a} = \frac{1}{x} + \frac{a}{x^2} + \frac{a^2}{x^3} + \ldots;$$

donc, en remplaçant successivement a par chacune des autres racines, et ajoutant ensemble tous les résultats, on aura

$$\frac{X'}{X} = \frac{m}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \ldots,$$

ou

$$\frac{xX'}{X} = m + \frac{s_1}{x} + \frac{s_2}{x^2} + \ldots.$$

Pour le calcul numérique, il sera plus commode d'éviter les exposants négatifs : on changera alors x en $\frac{1}{z}$, et la fraction $\frac{xX'}{X}$ sera de la forme $\frac{Z_1}{Z}$; on aura

$$\frac{Z_1}{Z} = m + s_1 z + s_2 z^2 + \ldots,$$

et l'on obtiendra toutes les sommes s_1, s_2, etc., par la division des polynômes Z_1 et Z que l'on ordonnera suivant les puissances croissantes de z.

On peut trouver de la même manière les sommes s_{-1},

s_{-2}, etc., des puissances semblables à exposants négatifs. Effectivement, si l'on développe la fonction $\frac{1}{x-a}$ suivant les puissances croissantes de x, il vient

$$\frac{1}{x-a} = -\left(\frac{1}{a} + \frac{x}{a^2} + \frac{x^2}{a^3} + \ldots\right),$$

donc, en remplaçant successivement a par chacune des autres racines et ajoutant les résultats, on aura

$$\frac{-X'}{X} = s_{-1} + s_{-2}\,x + s_{-3}\,x^2 + \ldots.$$

On obtiendra donc les sommes s_{-1}, s_{-2}, etc., en ordonnant les polynômes $-X'$ et X suivant les puissances croissantes de x et en effectuant ensuite la division du premier polynôme par le second.

Le principal avantage de cette seconde méthode basée sur la division algébrique, consiste en ce que l'on peut en déduire aisément l'expression générale de s_n ou de s_{-n} en fonction des coefficients de l'équation proposée (*voir* la Note I). Les formules de Newton ne conduiraient que péniblement au même résultat.

Détermination des fonctions symétriques doubles, triples, etc., des racines d'une équation.

Les formules établies précédemment permettent de calculer successivement les fonctions symétriques doubles, triples, etc., des racines d'une équation.

Soient $a, b, c, \ldots, k, l$ les m racines d'une équation

$$X = 0$$

de degré m, et considérons une fonction symétrique double, dont un terme soit $a^\alpha b^\beta$; la fonction dont il s'agit, étant déterminée quand on en connaît un terme, nous

la représenterons, pour abréger, par $\sum a^\alpha b^6$, et nous continuerons de désigner par s_α la somme des puissances $\alpha^{\text{ièmes}}$ de toutes les racines.

Cela posé, si l'on multiplie entre elles les deux sommes s_α et s_6, on voit aisément que le produit sera la somme des deux quantités $s_{\alpha+6}$ et $\sum a^\alpha b^6$; on aura donc

$$\sum a^\alpha b^6 = s_\alpha s_6 - s_{\alpha+6}.$$

On voit que toute fonction double $\sum a^\alpha b^6$ est exprimable, sous forme rationnelle et entière, par les coefficients de l'équation proposée, puisque s_α, s_6 et $s_{\alpha+6}$ le sont; et si les coefficients de l'équation sont des nombres entiers, $\sum a^\alpha b^6$ sera aussi un nombre entier.

La formule précédente n'a plus lieu si $6 = \alpha$; on voit, en effet, que si 6 devient égal à α, les termes de $\sum a^\alpha b^6$ sont égaux deux à deux, en sorte que cette quantité se réduit à $2\sum a^\alpha b^\alpha$; on aura donc

$$\sum a^\alpha b^\alpha = \frac{1}{2}\left[(s_\alpha)^2 - s_{2\alpha}\right].$$

En remplaçant s_α et $s_{2\alpha}$ par leurs valeurs, on aura la valeur de $\sum a^\alpha b^\alpha$ qui ne contiendra plus le dénominateur 2; mais cela ne se voit pas immédiatement; cette proposition résultera, comme nous le verrons dans la prochaine leçon, des méthodes données par Waring et par M. Cauchy, pour la détermination des fonctions symétriques des racines d'une équation.

Une fonction symétrique triple, dont un terme est $a^\alpha b^\beta c^\gamma$, pourra être représentée par $\sum a^\alpha b^\beta c^\gamma$. Si l'on multiplie la fonction double $\sum a^\alpha b^\beta$, que nous savons former par s_γ on trouvera pour produit

$$\sum a^\alpha b^\beta c^\gamma + \sum a^{\alpha+\gamma} b^\beta + \sum a^\alpha b^{\beta+\gamma};$$

on aura donc

$$\sum a^\alpha b^\beta c^\gamma = s_\gamma \sum a^\alpha b^\beta - \sum a^{\alpha+\gamma} b^\beta - \sum a^\alpha b^{\beta+\gamma}.$$

Cette formule fait connaître la fonction triple $\sum a^\alpha b^\beta c^\gamma$, car le second membre ne contient que des fonctions doubles que l'on sait calculer. Si l'on veut avoir la valeur de la fonction triple, au moyen des sommes de puissances semblables, il suffira de remplacer les fonctions doubles par leurs valeurs connues; on trouvera ainsi

$$\sum a^\alpha b^\beta c^\gamma = s_\alpha s_\beta s_\gamma - s_{\alpha+\beta} s_\gamma - s_{\alpha+\gamma} s_\beta - s_{\beta+\gamma} s_\alpha + 2 s_{\alpha+\beta+\gamma},$$

et l'on voit que les fonctions triples s'exprimeront comme les fonctions simples et doubles, sous forme rationnelle et entière, par les coefficients de l'équation proposée.

La relation précédente n'a plus lieu, si deux des exposants ou tous les trois deviennent égaux entre eux; mais on peut en déduire aisément les valeurs des deux fonctions

$$\sum a^\alpha b^\alpha c^\gamma \quad \text{et} \quad \sum a^\alpha b^\alpha c^\alpha.$$

On voit, en effet, que si β devient égal à α, $\sum a^\alpha b^\beta c^\gamma$ se réduit à $2 \sum a^\alpha b^\alpha c^\gamma$ et à $2.3 \sum a^\alpha b^\alpha c^\alpha$, si en même

temps γ devient égal à α; on aura donc

$$\sum a^\alpha b^\alpha c^\gamma = \frac{1}{2}(s_\alpha^2 s_\gamma - s_{2\alpha} s_\gamma - 2s_{\alpha+\gamma} s_\alpha + 2s_{2\alpha+\gamma})$$

et

$$\sum a^\alpha b^\alpha c^\alpha = \frac{1}{6}(s_\alpha^3 - 3s_{2\alpha} s_\alpha + 2s_{3\alpha}).$$

En suivant la même marche, on calculera successivement les fonctions du quatrième ordre, puis celles du cinquième, et ainsi de suite. Et on pourrait aussi déduire de là la formule qui fait connaître immédiatement l'expression d'une fonction symétrique d'ordre quelconque, en fonction des sommes de puissances semblables (*voir* la Note II). Il est presque superflu d'ajouter que quand on aura calculé, en général, l'expression d'une fonction symétrique entière et homogène du $n^{ième}$ ordre, si μ exposants deviennent égaux entre eux, il faudra diviser par $1.2.3\ldots\mu$ la valeur qu'on aura trouvée.

On voit, par là, que toute fonction symétrique entière et homogène des racines d'une équation peut s'exprimer rationnellement par les coefficients de cette équation, et que la même chose a lieu, d'après les remarques faites précédemment, pour une fonction symétrique rationnelle quelconque.

DEUXIÈME LEÇON.

Méthode de Waring pour calculer une fonction symétrique rationnelle et entière des racines d'une équation. — Méthode de M. Cauchy. — Application de la méthode de M. Cauchy à un exemple.

Méthode de Waring pour calculer une fonction symétrique rationnelle et entière des racines d'une équation.

Waring a indiqué, dans ses *Meditationes algebraicæ* (*), une méthode par laquelle on peut former directement l'expression d'une fonction symétrique et entière quelconque des racines d'une équation en fonction des coefficients de cette équation. Nous allons faire connaître ici cette méthode qui, dans un très-grand nombre de cas, devra être préférée à celle que nous avons exposée dans la leçon précédente.

Soit l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

dont les m racines sont

$$a,\ b,\ c,\ldots\, i,\ k,\ l,$$

et supposons qu'il s'agisse de trouver la valeur d'une fonction symétrique et entière V de ces racines.

Pour plus de clarté, il convient d'imaginer que l'on ait ordonné la fonction V de la manière que nous allons indiquer. Désignons par α l'exposant de la plus haute puis-

(*) *Editio tertia*, p. 13.

sance à laquelle se trouve élevée chaque racine, et, en particulier, la racine a dans V; par β l'exposant de la plus haute puissance à laquelle se trouve élevée la racine b dans la partie de V qui contient le facteur a^α; par γ l'exposant de la plus haute puissance à laquelle se trouve élevée c dans la partie de V qui renferme le facteur $a^\alpha b^\beta$; et ainsi de suite, en sorte que λ désignera finalement l'exposant de la plus haute puissance de l dans la partie de V qui contient le facteur $a^\alpha b^\beta c^\gamma \ldots k^\varkappa$. D'après cela, la fonction V contiendra un terme de la forme

$$A a^\alpha b^\beta c^\gamma \ldots k^\varkappa l^\lambda,$$

auquel nous assignerons le premier rang; A est une constante donnée; il se peut que quelques-uns des exposants

$$\alpha, \beta, \gamma, \ldots, \varkappa, \lambda$$

soient nuls; en outre, chacun de ces exposants peut être égal, mais non supérieur au précédent. Je dis, par exemple, qu'on ne peut avoir $\gamma > \beta$; en effet, la fonction symétrique V qui renferme le terme $A a^\alpha b^\beta c^\gamma \ldots k^\varkappa l^\lambda$ contiendra aussi le terme $A a^\alpha b^\gamma c^\beta \ldots k^\varkappa l^\lambda$, qui se déduit du premier en permutant les lettres b et c; or, si l'on avait $\gamma > \beta$, b^β ne serait pas, comme nous l'avons supposé, la plus haute puissance de b contenue dans la partie de V qui renferme le facteur a^α; donc on a nécessairement $\gamma < \beta$ ou $\gamma = \beta$. Ce raisonnement s'applique évidemment aux autres exposants.

Le premier terme de la fonction V ayant été fixé, comme il vient d'être dit, nous appliquerons la même règle à la détermination du rang de chacun des autres termes, et nous écrirons :

$$V = A a^\alpha b^\beta c^\gamma \ldots k^\varkappa l^\lambda + \ldots.$$

Cela posé, on a, en conservant les notations de la leçon précédente :

$$(-1)\, p_1 = \sum a,$$

$$(-1)^2 p_2 = \sum ab,$$

$$(-1)^3 p_3 = \sum abc,$$

$$\dots\dots\dots\dots$$

$$\dots\dots\dots\dots$$

$$(-1)^{m-1} p_{m-1} = \sum abc\dots k,$$

$$(-1)^m p_m = abc\dots kl.$$

Si l'on élève ces égalités aux puissances

$$\alpha - \beta,\quad \beta - \gamma, \dots,\quad \varkappa - \lambda,\ \lambda$$

respectivement, qu'on en fasse ensuite le produit et qu'on multiplie enfin de part et d'autre par A, le premier membre de l'égalité résultante sera

$$A(-1)^{\alpha+\beta+\gamma+\dots+\lambda} p_1^{\alpha-\beta} p_2^{\beta-\gamma} \dots p_{m-1}^{\varkappa-\lambda} p_m^{\lambda},$$

nous le représenterons, pour abréger, par P; quant au second membre, il sera une fonction symétrique des lettres $a, b, c, \dots, k, l$, et, si nous l'ordonnons de la même manière que V, il est évident que son premier terme sera $A\, a^\alpha b^\beta c^\gamma \dots k^\varkappa l^\lambda$; on aura ainsi

$$P = A\, a^\alpha b^\beta c^\gamma \dots k^\varkappa l^\lambda + \dots.$$

En retranchant la seconde des fonctions symétriques V et P de la première, on obtient une nouvelle fonction symétrique V_1 telle que

$$V - P = V_1.$$

Si l'on opère sur V_1 comme on a opéré sur V, on ob-

tiendra une nouvelle fonction symétrique V_2 telle que

$$V_1 - P_1 = V_2;$$

P_1 désigne une quantité analogue à P, et qui est, comme celle-ci, le produit d'une constante par diverses puissances des coefficients $p_1, p_2, \ldots, p_m$.

En poursuivant ces opérations, on voit qu'on obtiendra une suite de fonctions symétriques,

$$V_1,\ V_2,\ V_3, \ldots,\ V_{\mu-1},\ V_\mu,$$

telles que

$$\begin{aligned} V - P &= V_1, \\ V_1 - P_1 &= V_2, \\ V_2 - P_2 &= V_3, \\ &\ldots\ldots\ldots\ldots \\ V_{\mu-2} - P_{\mu-2} &= V_{\mu-1}, \\ V_{\mu-1} - P_{\mu-1} &= V_\mu; \end{aligned}$$

chacune des quantités $P, P_1, \ldots, P_\mu$ est le produit d'une constante par diverses puissances des coefficients p_1, $p_2, \ldots, p_m$. En outre, si l'on imagine une fonction entière U formée des premiers termes des fonctions $V, V_1, \ldots, V_\mu$ et ordonnée de la même manière que ces fonctions, il est évident, d'après le procédé que nous avons suivi, que le premier terme de l'une quelconque des fonctions V_1, $V_2, \ldots, V_\mu$ occupera, dans U, un rang supérieur au rang du premier terme de la fonction précédente. Or, le nombre des termes susceptibles d'occuper, dans U, un rang supérieur à celui d'un terme donné est nécessairement limité; donc, dans la recherche des fonctions $V_1, V_2, \ldots$, on finira toujours par arriver à une constante, et alors l'opération sera terminée. Supposons, d'après cela, que V_μ se réduise à une constante; il vient, en ajoutant les

égalités précédentes,

$$V = P + P_1 + P_2 + \ldots + P_{\mu-1} + V_\mu,$$

formule qui fait connaître l'expression de la fonction symétrique proposée V en fonction des coefficients p_1, $p_2, \ldots, p_m$.

On voit, par ce résultat, que toute fonction entière et symétrique V des racines d'une équation est exprimable rationnellement par les coefficients de l'équation, proposition que nous avons déjà établie dans la leçon précédente. Mais on voit, en outre, que si les coefficients de l'équation sont des nombres entiers, ainsi que ceux qui multiplient les différents termes de V, la valeur de cette fonction V sera également un nombre entier.

Exemple I. — Étant donnée l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

dont $a, b, c, d, e, f, \ldots, k, l$ sont les racines, on demande la valeur de la fonction symétrique

$$V = \sum a^3 b^2 c.$$

Posons, conformément à la théorie précédente,

$$P = p_1 p_2 p_3 = \sum a . \sum ab . \sum abc$$

$$= \sum a^3 b^2 c + 3 \sum a^3 bcd + 3 \sum a^2 b^2 c^2 + 8 \sum a^2 b^2 cd$$

$$+ 22 \sum a^2 bcde + 60 \sum abcdef,$$

on aura

$$V - P = V_1 = -3 \sum a^3 bcd - 3 \sum a^2 b^2 c^2 - 8 \sum a^2 b^2 cd$$

$$- 22 \sum a^2 bcde - 60 \sum abcdef;$$

faisons, en second lieu,

$$P_1 = -3p_1^2 p_4 = -3\left[\sum a\right]^2 \sum abcd$$

$$= -3\sum a^3bcd - 6\sum a^2b^2cd - 27\sum a^2bcde - 90\sum abcdef,$$

on aura

$$V_1 - P_1 = V_2 = -3\sum a^2b^2c^2 - 2\sum a^2b^2cd$$

$$+ 5\sum a^2bcde + 30\sum abcdef;$$

faisons, en troisième lieu,

$$P_2 = -3p_3^2 = -3\left[\sum abc\right]^2$$

$$= -3\sum a^2b^2c^2 - 6\sum a^2b^2cd - 18\sum a^2bcde - 60\sum abcdef,$$

on aura

$$V_2 - P_2 = V_3 = 4\sum a^2b^2cd + 23\sum a^2bcde + 90\sum abcdef;$$

faisons, en quatrième lieu,

$$P_3 = 4p_2p_4 = 4\sum ab\sum abcd$$

$$= 4\sum a^2b^2cd + 16\sum a^2bcde + 60\sum abcdef,$$

on aura

$$V_3 - P_3 = V_4 = 7\sum a^2bcde + 30\sum abcdef;$$

faisons, en cinquième lieu,

$$P_4 = 7p_1p_5 = 7\sum a\sum abcde$$

$$= 7\sum a^2bcde + 42\sum abcdef,$$

on aura

$$V_4 - P_4 = V_5 = -12 \sum abcdef;$$

si enfin l'on fait

$$P_5 = -12 p_6 = -12 \sum abcdef,$$

on aura

$$V_5 - P_5 = V_6 = 0.$$

Ici l'opération est terminée et l'on a cette valeur de V,

$$V = p_1 p_2 p_3 - 3 p_1^2 p_4 - 3 p_3^2 + 4 p_2 p_4 + 7 p_1 p_5 - 12 p_6.$$

Exemple II. — Étant donnée l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

dont $a, b, c, \ldots, k, l$, sont les racines, on demande la valeur de la fonction symétrique

$$\sum a^2 b^2 \ldots f^2 g \ldots h;$$

μ est le nombre des racines qui entrent au carré dans chaque terme, et ν le nombre de celles qui entrent à la première puissance.

Désignons la fonction proposée par la notation $F(\mu, \nu)$, et, plus généralement, représentons par $F(\mu - n, \nu + 2n)$ la fonction symétrique de même genre que la proposée et dont chaque terme contient $\mu - n$ racines au carré et $\nu + 2n$ racines à la première puissance.

Cela posé, on doit former, d'après notre théorie, les $\mu + 1$ égalités suivantes :

$$(-1)^\nu p_\mu p_{\nu+\mu} = F(\mu, \nu) + \frac{\nu + 2}{1} F(\mu - 1, \nu + 2)$$
$$+ \frac{(\nu + 4)(\nu + 3)}{1.2} F(\mu - 2, \nu + 4) + \ldots\ldots$$
$$+ \frac{(\nu + 2n)(\nu + 2n - 1)\ldots(\nu + n + 1)}{1.2\ldots n} F(\mu - n, \nu + 2n) + \ldots$$
$$+ \frac{(\nu + 2\mu)\ldots(\nu + \mu + 1)}{1.2\ldots\mu} F(0, \nu + 2\mu);$$

$$(-1)^\nu p_{\mu-1} p_{\nu+\mu+1} = F(\mu-1,\ \nu+2)$$
$$+ \frac{\nu+4}{1} F(\mu-2,\ \nu+4) + \frac{(\nu+6)(\nu+5)}{1.2} F(\mu-3,\ \nu+6) + \ldots$$
$$+ \frac{(\nu+2n)\ldots(\nu+n+2)}{1.2\ldots(n-1)} F(\mu-n,\ \nu+2n) + \ldots$$
$$+ \frac{(\nu+2\mu)\ldots(\nu+\mu+2)}{1.2\ldots(\mu-1)} F(0,\ \nu+2\mu),$$

. . . . ;

$$(-1)^\nu p_{\mu-n} p_{\nu+\mu+n} = F(\mu-n,\ \nu+2n) + \ldots$$
$$+ \frac{(\nu+2\mu)\ldots(\nu+\mu+n+1)}{1.2\ldots(\mu-n)} F(0,\ \nu+2\mu)$$

. . . . ;

$$(-1)^\nu p_1 p_{\nu+2\mu-1} = F(1,\ \nu+2\mu-2) + \frac{\nu+2\mu}{1} F(0,\ \nu+2\mu),$$
$$(-1)^\nu p_{\nu+2\mu} = F(0,\ \nu+2\mu).$$

Ajoutons toutes ces égalités après les avoir multipliées respectivement par les facteurs

$$1,\ \lambda_1,\ \lambda_2, \ldots,\ \lambda_n, \ldots,\ \lambda_\mu,$$

et supposons ces facteurs choisis de manière que les quantités

$$F(\mu-1,\ \nu+2),\quad F(\mu-2,\ \nu+4), \ldots,\ F(0,\ \nu+2\mu)$$

soient éliminées du résultat, il viendra

$$F(\mu,\nu) = (-1)^\nu \left(\begin{array}{l} p_\mu p_{\nu+\mu} + \lambda_1 p_{\mu-1} p_{\nu+\mu+1} + \ldots \\ + \lambda_n p_{\mu-n} p_{\nu+\mu+n} + \ldots + \lambda_\mu p_{\nu+2\mu} \end{array} \right).$$

Nous allons chercher maintenant les valeurs des facteurs $\lambda_1, \lambda_2, \ldots, \lambda_\mu$. Les équations qui déterminent ces facteurs s'obtiennent en donnant à n les μ valeurs $1,\ 2,$

$3, \ldots, \mu$, dans la suivante :

$$\lambda_n + \frac{\nu+2n}{1}\lambda_{n-1} + \frac{(\nu+2n)(\nu+2n-1)}{1.2}\lambda_{n-2}$$
$$+ \frac{(\nu+2n)(\nu+2n-1)((\nu+2n-2)}{1.2.3}\lambda_{n-3} + \ldots\ldots$$
$$+ \frac{(\nu+2n)(\nu+2n-1)\ldots(\nu+2n-r+1)}{1.2\ldots r}\lambda_{n-r} + \ldots$$
$$+ \frac{(\nu+2n)\ldots(\nu+n+1)}{1.2\ldots n} = 0;$$

mais cette équation peut s'écrire d'une autre manière. Posons, pour abréger,

$$\theta_\rho = \frac{(\nu+2\rho)(\nu+\rho-1)}{(\nu+2\rho-2)\rho},$$

et

$$A_\rho = \frac{n-\rho}{(\nu+2n-2\rho)n}\,\frac{(\nu+2n)(\nu+2n-1)\ldots(\nu+2n-\rho)}{1.2.3\ldots\rho},$$

on aura

$$\frac{\nu+2n}{1} = \theta_n + A_1,$$

et généralement

$$\frac{(\nu+2n)(\nu+2n-1)\ldots(\nu+2n-r+1)}{1.2.3\ldots r} = A_{r-1}\,\theta_{n-r+1} + A_r.$$

D'après cela, notre équation devient, en remarquant que A_n est nul,

$$(\lambda_n + \theta_n\lambda_{n-1}) + A_1(\lambda_{n-1} + \theta_{n-1}\lambda_{n-2}) + A_2(\lambda_{n-2} + \theta_{n-2}\lambda_{n-3}) + \ldots$$
$$+ A_{n-2}(\lambda_2 + \theta_2\lambda_1) + A_{n-1}(\lambda_1 + \theta_1) = 0.$$

En donnant successivement à n les valeurs $1, 2, 3, \ldots, n$, on obtient n équations, d'où l'on tire immédiatement

$$\lambda_1 + \theta_1 = 0,\quad \lambda_2 + \theta_2\lambda_1 = 0,\quad \lambda_3 + \theta_3\lambda_2, \ldots, \lambda_n + \theta_n\lambda_{n-1} = 0,$$

ou

$$\lambda_1 = -(\nu + 2),$$
$$\lambda_2 = -\frac{(\nu+4)(\nu+1)}{(\nu+2).2}\lambda_1,$$
$$\lambda_3 = -\frac{(\nu+6)(\nu+2)}{(\nu+4).3}\lambda_2,$$
$$\dots\dots\dots\dots\dots\dots$$
$$\dots\dots\dots\dots\dots\dots$$
$$\lambda_n = -\frac{(\nu+2n)(\nu+n-1)}{(\nu+2n-2).n}\lambda_{n-1}.$$

En multipliant ces égalités membre à membre, il vient

$$\lambda_n = (-1)^n \frac{(\nu+1)(\nu+2)\dots(\nu+n-1)}{1.2\dots(n-1)} \cdot \frac{\nu+2n}{n},$$

ce qui permet d'écrire immédiatement la valeur de la fonction symétrique cherchée $F(\mu, \nu)$.

Il faut remarquer que notre procédé est en défaut dans le cas de $\nu = 0$, mais la formule qui fait connaître λ_n ne cesse pas toutefois d'être exacte. Dans le cas dont il s'agit, les valeurs de θ_ρ et de A_ρ deviennent

$$\theta_\rho = 1, \quad A_\rho = \frac{(2n-1)(2n-2)\dots(2n-\rho)}{1.2\dots\rho};$$

on voit que A_n n'est pas nul, comme dans le cas général, et qu'il est ici égal à A_{n-1}. L'équation entre λ_n, $\lambda_{n-1}, \dots, \lambda_1$ peut alors s'écrire ainsi :

$$(\lambda_n + \lambda_{n-1}) + A_1(\lambda_{n-1} + \lambda_{n-2}) + \dots + A_{n-2}(\lambda_2 + \lambda_1)$$
$$+ A_{n-1}(\lambda_1 + 2) = 0;$$

en remplaçant successivement n par $1, 2, \dots, n$, on obtient n équations, d'où l'on tire immédiatement

$$\lambda_1 + 2 = 0, \quad \lambda_2 + \lambda_1 = 0, \quad \lambda_3 + \lambda_2 = 0, \dots, \lambda_n + \lambda_{n-1} = 0,$$

et, par suite,

$$\lambda_n = (-1)^n . 2;$$

on a donc cette valeur de $F(\mu, o)$,

$$F(\mu, o) = p_{\mu}^2 - 2p_{\mu-1}p_{\mu+1} + 2p_{\mu-2}p_{\mu+2} - \ldots \pm 2p_1 p_{2\mu-1} \mp 2p_{2\mu}.$$

Méthode de M. Cauchy.

M. Cauchy a publié, dans ses anciens *Exercices de Mathématiques* (4e année, page 103), une méthode nouvelle et fort élégante pour trouver la valeur d'une fonction symétrique et entière des racines d'une équation. Cette méthode consiste à éliminer successivement de l'expression de la fonction symétrique qu'on veut évaluer, chacune des racines de l'équation proposée; elle repose sur la proposition suivante :

Soit V une fonction symétrique et entière des racines $a, b, c, \ldots, i, k, l$ d'une équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

que nous représenterons aussi, pour abréger, par

$$X = 0;$$

et supposons qu'ayant éliminé de l'expression de V, par un moyen quelconque, toutes les racines excepté a, on ait mis la valeur de cette fonction sous la forme d'un polynôme entier et rationnel ordonné par rapport aux puissances de a, que l'on ait, par exemple,

$$V = A_0 a^{\mu} + A_1 a^{\mu-1} + \ldots + A_{\mu-1} a + A_{\mu},$$

A_0, A_1, etc., étant des quantités composées rationnellement avec les coefficients de l'équation proposée; je dis que si l'on divise cette expression de V par le polynôme

$$A = a^m + p_1 a^{m-1} + p_2 a^{m-2} + \ldots + p_{m-1} a + p_m,$$

obtenu en remplaçant x par a dans X, le reste de la divi-

sion ne contiendra pas a, et sera précisément la valeur de la fonction V.

En effet, si Q et R désignent le quotient et le reste de la division V par A, on aura $V = AQ + R$, et comme A est nul,

$$V = R.$$

D'ailleurs, ce reste R est au plus du degré $m-1$ en a; nous le représenterons par

$$q_0 a^{m-1} + q_1 a^{m-2} + \ldots + q_{m-2} a + q_{m-1},$$

et l'on aura

$$V = q_0 a^{m-1} + q_1 a^{m-2} + \ldots + q_{m-2} a + q_{m-1}.$$

Mais V étant une fonction symétrique, on peut changer a et b l'un dans l'autre, ainsi que a et c, etc.; et, comme par ces changements, q_0, q_1, etc., conservent leurs valeurs, il s'ensuit que l'équation

$$q_0 x^{m-1} + q_1 x^{m-2} + \ldots + q_{m-2} x + (q_{m-1} - V) = 0$$

sera satisfaite en remplaçant x par l'une quelconque des m racines $a, b, \ldots, k, l$; ce qui est impossible, à moins que les coefficients ne soient tous nuls, puisque cette équation n'est que du degré $m-1$: on aura donc, en particulier,

$$q_{m-1} - V = 0,$$

ou

$$V = q_{m-1},$$

comme nous l'avions annoncé.

La démonstration précédente suppose que les m racines $a, b, c, \ldots, k, l$ sont toutes inégales; mais les conclusions précédentes ne subsistent pas moins, si quelques-unes de ces racines sont égales entre elles. Nous emploierons, pour justifier cette assertion, un raisonnement dont on fait un fréquent usage en analyse.

Si l'équation $X = 0$ a des racines égales, on considérera d'abord à sa place une équation $X_1 = 0$, dont toutes les racines seront inégales, et qu'on obtiendra en faisant subir des modifications insensibles aux coefficients de X; par exemple, si l'équation $X = 0$ a trois racines égales à a, et que les autres racines soient différentes, on prendra

$$X_1 = \frac{X(x-a-h)(x-a-h')}{(x-a)^2}.$$

Le polynôme X_1 ne diffère de X qu'en ce que deux des trois racines égales à a sont remplacées par $a+h$ et $a+h'$: on voit aisément, sans qu'il soit nécessaire d'insister davantage, comment on devrait choisir le polynôme X_1, si, outre les trois racines égales à a, l'équation proposée avait plusieurs racines égales à b, à c, etc. Cela posé, substituant l'équation $X_1 = 0$ à $X = 0$, et conservant d'ailleurs les notations précédentes, on arrivera à l'équation

$$V = q_{m-1},$$

et cette équation aura lieu, quelque petites que soient les quantités h, h', etc.; elle aura donc lieu aussi à la limite, c'est-à-dire quand on fera $h = 0$, $h' = 0$, etc.

Voici maintenant quelle est la méthode donnée par M. Cauchy, pour calculer la valeur d'une fonction V symétrique et entière des racines $a, b, c, \ldots, i, k, l$ de l'équation

$$X = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_m = 0.$$

Divisons X par $x - a$, et désignons par X_1 le quotient; divisons de même X_1 par $x - b$, et désignons par X_2 le quotient, puis X_2 par $x - c$, et soit X_3 le quotient, et continuons ainsi d'enlever de X tous les facteurs linéaires jusqu'à $x - k$ inclusivement, en sorte que X_{m-1} ne con-

tiendra plus que le seul facteur $x - l$. Cela posé, considérons les m équations

$$X = 0, \quad X_1 = 0, \quad X_2 = 0, \ldots, \quad X_{m-1} = 0.$$

La première n'est autre que la proposée, et a pour racines $a, b, c, \ldots, k, l$; la seconde a pour racines $b, c, \ldots, k, l$, et ses coefficients sont exprimés sous forme entière en fonction de a et des coefficients de la proposée; la troisième a pour racines $c, \ldots, k, l$, et ses coefficients sont exprimés sous forme entière en fonction de b et des coefficients de la précédente, c'est-à-dire en fonction de a, b et des coefficients de la proposée; et, en général, les coefficients de l'une quelconque de ces équations sont exprimés sous forme entière en fonction des coefficients de la proposée et des racines qui n'appartiennent pas à l'équation que l'on considère. Désignons enfin par A la valeur de X pour $x = a$, par B la valeur de X_1 pour $x = b$, par C celle de X_2 pour $x = c$, et ainsi de suite, en sorte que I sera la valeur de X_{m-3} pour $x = i$, K celle de X_{m-2} pour $x = k$, et L celle de X_{m-1} pour $x = l$; on aura

$$A = 0, \quad B = 0, \quad C = 0, \ldots, \quad I = 0, \quad K = 0, \quad L = 0.$$

Cela posé, V est une fonction symétrique, non-seulement des racines de l'équation $X = 0$, mais aussi des racines de l'une quelconque des équations

$$X = 0, \quad X_1 = 0, \ldots, \quad X_{m-3} = 0, \quad X_{m-2} = 0, \quad X_{m-1} = 0.$$

Nous allons faire voir comment, en s'appuyant sur cette remarque, on peut, à l'aide du théorème fondamental démontré plus haut, éliminer successivement chaque racine de l'expression de V.

D'abord l'équation $L = 0$, où l entre au premier degré, permet de chasser immédiatement l de l'expression de V.

Considérant alors V comme fonction symétrique des deux racines k et l de l'équation $X_{m-2} = 0$, dont l'une l est déjà éliminée, on l'ordonnera par rapport à k, et on la divisera par K, conformément à ce qui a été dit plus haut; le reste de la division ne contiendra pas k et sera la valeur de V débarrassée des racines k et l. On considérera alors V comme fonction symétrique des trois racines i, k, l de l'équation $X_{m-3} = 0$, dont les deux dernières n'entrent plus dans son expression, et l'ayant ordonnée par rapport à i, on la divisera par I à l'effet d'éliminer i; le reste de la division ne contiendra pas i et sera la valeur de V débarrassée des trois racines i, k, l. On continuera de la même manière, jusqu'à ce qu'on ait éliminé de V chacune des racines a, b, c,..., i, k, l; on aura alors la valeur de cette fonction exprimée par les coefficients de l'équation proposée.

Il importe de remarquer que l'expression définitive de V s'obtient par de simples divisions, et que les premiers termes des polynômes A, B, C,..., I, K, L, qui servent successivement de diviseurs, ont tous l'unité pour coefficient: par conséquent, ces divisions n'introduiront aucun dénominateur; en sorte que si l'expression primitive de V est entière, non-seulement par rapport aux racines a, b, c,..., i, k, l, qui y entrent symétriquement, mais aussi par rapport aux coefficients p_1, p_2, etc., qui peuvent aussi y entrer, l'expression définitive de V sera aussi entière par rapport à ces coefficients; et enfin, si ces coefficients sont des nombres entiers, V sera lui-même un nombre entier. Ce théorème important, que nous n'avions pas établi complétement par la méthode exposée dans la leçon précédente, mais qui résulte immédiatement de la méthode de Waring, se déduit aussi, comme on voit, de la méthode de M. Cauchy.

Application de la méthode de M. Cauchy à un exemple.

Nous allons appliquer la méthode de M. Cauchy à la détermination du produit des carrés de toutes les différences des racines d'une équation donnée, prises deux à deux. Cet exemple suffira pour montrer comment on peut, par des artifices convenables, simplifier dans certains cas l'emploi de la méthode.

Soient toujours $a, b, c, \ldots, k, l$ les m racines de l'équation

$$(1)\quad X = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0;$$

soient aussi

$$V = (a-b)^2 (a-c)^2 \ldots\ldots\ldots\ldots (k-l)^2$$

et

$$V_1 = (b-c)^2 (b-d)^2 \ldots\ldots\ldots\ldots (k-l)^2;$$

V sera le produit des carrés des différences des racines de l'équation (1), prises deux à deux, et V_1 le produit des carrés des différences des racines de l'équation

$$\frac{X}{x-a} = 0,$$

ou

$$(2)\quad \begin{array}{l|l|l} x^{m-1} + p_1 & x^{m-2} + p_2 & x^{m-3} + \ldots + a^{m-1} = 0, \\ \quad\;\; + a & \quad\;\; + p_1 a & \qquad\qquad\;\; + p_1 a^{m-2} \\ & \quad\;\; + a^2 & \qquad\qquad\;\; + \ldots\ldots\ldots \\ & & \qquad\qquad\;\; \ldots\ldots\ldots\ldots \\ & & \qquad\qquad\;\; + p_{m-1}. \end{array}$$

Cela posé, on a

$$V = V_1 (a-b)^2 (a-c)^2 \ldots (a-k)^2 (a-l)^2.$$

Mais le produit $(a-b)(a-c)\ldots(a-k)(a-l)$ est, comme on sait, égal à la valeur que prend la dérivée du polynôme X pour $x=a$, c'est-à-dire à

$$ma^{m-1}+(m-1)p_1a^{m-2}+\ldots+p_{m-1};$$

donc on aura

$$V=V_1[ma^{m-1}+(m-1)p_1a^{m-2}+\ldots+p_{m-1}]^2.$$

Si donc nous admettons qu'on sache former la valeur de la fonction V pour une équation du degré $m-1$, on pourra également trouver la valeur de cette fonction pour une équation du degré m. Effectivement, par hypothèse, on sait exprimer la valeur de V_1 par les coefficients de l'équation (2), c'est-à-dire en fonction de a et des coefficients de la proposée; donc la fonction V pourra ellemême être mise sous la forme d'un polynôme ordonné par rapport aux puissances de a, et, en divisant ce polynôme par le premier membre de l'équation proposée, dans lequel on aura remplacé x par a, le reste de la division donnera la valeur cherchée de V.

Or on sait calculer la fonction V pour une équation du second degré; on pourra donc calculer cette fonction pour l'équation du troisième degré, puis pour celle du quatrième, et ainsi de suite.

Cas de l'équation du troisième degré. — L'équation proposée est

$$x^3+px^2+qx+r=0,$$

et l'on a

$$V=(a-b)^2(a-c)^2(b-c)^2,$$

$$V_1=(b-c)^2,$$

$$V=V_1(a-b)^2(a-c)^2;$$

V_1 étant relatif à l'équation du deuxième degré

$$\begin{array}{r|l} x^2 + p & x + q = 0. \\ + a & + pa \\ & + a^2 \end{array}$$

On a immédiatement

$$V_1 = (p+a)^2 - 4(q + pa + a^2) = -3a^2 - 2pa + (p^2 - 4q);$$

d'ailleurs

$$(a-b)(a-c) = 3a^2 + 2pa + q,$$

par suite,

$$\begin{array}{l} V = (-3a^2 - 2pa + p^2 - 4q)(3a^2 + 2pa + q)^2 \\ = -27a^6 - 54pa^5 \begin{array}{r|r|r|r|l} -27p^2 & a^4 + 4p^3 & a^3 + 4p^4 & a^2 + 4p^3q & a + p^2q^2. \\ -54q & -72pq & -18p^2q & -18pq^2 & -4q^3 \\ & & -27q^2 & & \end{array} \end{array}$$

Divisant cette valeur de V par $a^3 + pa^2 + qa + r$, on trouve pour quotient

$$-27a^3 - 27pa^2 - 27qa + (4p^3 + 27r - 18pq),$$

et pour reste,

$$-4q^3 - 27r^2 + 18pqr + p^2q^2 - 4p^3r,$$

ce qui est précisément la valeur de V que nous cherchons. On trouvera dans la Note III une méthode plus expéditive pour résoudre la même question.

TROISIÈME LEÇON.

Formation de l'équation de laquelle dépend une fonction rationnelle et non symétrique des racines d'une équation donnée. — Équation aux carrés des différences. — Sur la forme des fonctions rationnelles d'une ou de plusieurs racines d'une équation. — Méthode d'élimination fondée sur la théorie des fonctions symétriques. — Théorème sur le degré de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations.

Formation de l'équation de laquelle dépend une fonction rationnelle et non symétrique des racines d'une équation donnée.

Soient $a, b, c, \ldots, k, l$ les m racines d'une équation donnée $X = 0$, et

$$V = F(a, b, c, \ldots)$$

une fonction rationnelle donnée de ces racines, ou de quelques-unes d'entre elles. La théorie des fonctions symétriques conduit à une méthode très-simple et très-élégante pour former l'équation dont V dépend. Nous allons développer ici cette méthode.

Si la fonction V contient n des m racines, le plus grand nombre de valeurs qu'elle puisse avoir en échangeant les lettres $a, b, c, \ldots, k, l$ les unes dans les autres de toutes les manières possibles, sera évidemment égal au nombre des arrangements de m lettres n à n, c'est-à-dire à

$$m(m-1)(m-2)\ldots(m-n+1).$$

Mais il peut arriver que le nombre des valeurs distinctes de V soit beaucoup moindre; nous désignerons par μ ce nombre de valeurs, et par

$$V_1,\ V_2,\ V_3, \ldots,\ V_\mu$$

les μ valeurs de V. L'équation en V sera alors

$$(V - V_1)(V - V_2)\ldots(V - V_\mu) = 0,$$

ou

$$V^\mu + P_1 V^{\mu-1} + P_2 V^{\mu-2} + \ldots + P_{\mu-1} V + P_\mu = 0,$$

en posant

$$V_1 + V_2 + \ldots + V_\mu = -P_1,$$
$$V_1 V_2 + \ldots\ldots\ldots = P_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$V_1 V_2 \ldots V_\mu = \pm P_\mu.$$

Or les quantités $P_1, P_2, \ldots, P_\mu$ sont des fonctions symétriques des quantités V_1, V_2, etc., et, par suite, elles sont aussi des fonctions symétriques des racines a, b, c, etc., de l'équation proposée : on pourra donc calculer les coefficients de l'équation en V par l'une des méthodes que nous avons exposées dans les leçons précédentes.

Nous avons admis comme évident que toute fonction symétrique des quantités V_1, V_2, etc., est aussi une fonction symétrique des racines a, b, c, etc. Voici, au surplus, un moyen très-facile de le démontrer.

Par hypothèse, les quantités

(1) $$V_1, V_2, \ldots, V_\mu$$

sont toutes distinctes, et ce sont les seules valeurs que V puisse avoir. Cela posé, faisons subir aux lettres

$$a, b, c, \ldots, k, l$$

une permutation quelconque, et supposons que V_1 se change en V'_1, V_2 en V'_2, etc.; les quantités

(2) $$V'_1, V'_2, \ldots, V'_\mu$$

devront toutes se trouver dans la série V_1, V_2, etc., puisque cette dernière comprend toutes les valeurs de V; je dis, de plus, que tous les termes de la série (2) sont dif-

férents, et, par suite, sont les mêmes que ceux de la série (1) : on ne peut avoir, par exemple, $V'_1 = V'_2$, car V_1 et V_2 ne diffèrent de V'_1 et V'_2 qu'en ce que les quantités dont ces fonctions dépendent y sont désignées par des lettres différentes, et l'égalité $V'_1 = V'_2$ entraînerait, par conséquent, $V_1 = V_2$, ce qui est contre l'hypothèse. Il résulte de là que, si l'on fait subir aux lettres a, b, c, etc., un changement quelconque, les quantités V_1, V_2, etc., ne feront que s'échanger les unes dans les autres ; par suite, une fonction symétrique de ces fonctions ne sera pas changée, et sera aussi symétrique par rapport aux quantités $a, b, c, \ldots, k, l$.

On peut dans bien des cas simplifier, par des artifices particuliers, le calcul de l'équation en V ; on en verra un exemple dans la recherche de l'équation qui a pour racines les carrés des différences des racines d'une équation donnée, prises deux à deux.

Équation aux carrés des différences.

Soient toujours $a, b, c, \ldots, k, l$ les m racines d'une équation $X = 0$, et posons

$$V = (a - b)^2;$$

l'équation en V sera du degré $\frac{m(m-1)}{2} = \mu$, qui est le nombre des combinaisons de m lettres deux à deux, puisque la fonction V est symétrique par rapport aux deux lettres qu'elle contient. Si l'on suppose que cette équation soit

$$V^\mu + P_1 V^{\mu-1} + P_2 V^{\mu-2} + \ldots = 0,$$

il suffira de calculer les quantités P_1, P_2, etc., qui sont des fonctions symétriques des racines de l'équation proposée : or ces coefficients P_1, P_2, etc., seront immédiatement donnés par les formules de Newton, si l'on connait

les sommes des puissances semblables S_1, S_2,..., S_μ des racines de l'équation en V. Tout est donc ramené à calculer ces dernières sommes en fonction des coefficients de l'équation proposée, ou en fonction des sommes s_1, s_2, etc., des puissances semblables de ses racines, puisque les sommes s_1, s_2, etc., s'expriment par les coefficients, à l'aide des formules de Newton.

Voici le procédé indiqué par Lagrange pour calculer les sommes S_1, S_2, etc., relatives à l'équation en V, au moyen des sommes s_1, s_2, etc., relatives à l'équation proposée.

Posons

$$\varphi(x) = (x-a)^{2n} + (x-b)^{2n} + \ldots + (x-l)^{2n};$$

en donnant à x successivement les valeurs $a, b, c, \ldots, k, l$, et ajoutant tous les résultats, on aura

$$\begin{aligned}\varphi(a)+\varphi(b)+\ldots+\varphi(l) = {} & (a-b)^{2n}+\ldots+(a-l)^{2n} \\ & + (b-a)^{2n}+\ldots+(b-l)^{2n} \\ & + \ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots \\ & + (l-a)^{2n}+(l-b)^{2n}\ldots\end{aligned}$$

Or le second membre de cette équation est évidemment égal à $2S_n$; donc

$$2S_n = \varphi(a) + \varphi(b) + \ldots + \varphi(l).$$

D'un autre côté, en développant les différents termes de $\varphi(x)$, on trouve

$$\begin{aligned}\varphi(x) = {} & x^{2n} - 2nax^{2n-1} + \frac{2n(2n-1)}{1.2}a^2x^{2n-2} - \ldots + a^{2n} \\ & + x^{2n} - 2nbx^{2n-1} + \frac{2n(2n-1)}{1.2}b^2x^{2n-2} - \ldots + b^{2n} \\ & + \ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots \\ & + x^{2n} - 2nlx^{2n-1} + \frac{2n(2n-1)}{1.2}l^2x^{2n-2} - \ldots + l^{2n},\end{aligned}$$

ou

$$\varphi(x) = mx^{2n} - 2ns_1 x^{2n-1} + \frac{2n(2n-1)}{1.2} s_2 x^{2n-2} - \ldots + s_{2n}.$$

Remplaçant x successivement par a, b, c,..., l, et ajoutant tous les résultats, on aura la valeur suivante de $\varphi(a) + \varphi(b) + \ldots + \varphi(l)$ ou de $2S_n$,

$$2S_n = ms_{2n} - 2ns_1 s_{2n-1} + \frac{2n(2n-1)}{1.2} s_2 s_{2n-2} - \ldots + ms_{2n}.$$

On voit aisément que les termes à égale distance des extrêmes sont égaux dans le second membre; par suite, on aura cette valeur de S_n,

$$S_n = ms_{2n} - 2ns_1 s_{2n-1} + \frac{2n(2n-1)}{1.2} s_2 s_{2n-2} - \ldots$$

$$\pm \frac{1}{2} \frac{2n(2n-1)\ldots(n+1)}{1.2.3\ldots n} s_n s_n.$$

En donnant à n les valeurs successives 1, 2, 3,..., μ, on connaîtra les sommes S_1, S_2,..., S_μ dont on a besoin; on achèvera ensuite le calcul, comme nous l'avons indiqué précédemment.

Cas de l'équation du troisième degré. — Prenons pour exemple l'équation du troisième degré

$$x^3 + px^2 + qx + r = 0,$$

et soit

$$V^3 + PV^2 + QV + R = 0$$

l'équation aux carrés des différences.

On trouve

$$s_1 = -p,$$
$$s_2 = p^2 - 2q,$$
$$s_3 = -p^3 + 3pq - 3r,$$
$$s_4 = p^4 - 4p^2q + 4pr + 2q^2,$$
$$s_5 = -p^5 + 5p^3q - 5p^2r - 5pq^2 + 5qr,$$
$$s_6 = p^6 - 6p^4q + 6p^3r + 9p^2q^2 - 12pqr - 2q^3 + 3r^2;$$

puis,

$$S_1 = 3s_2 - s_1^2 = 2p^2 - 6q,$$
$$S_2 = 3s_4 - 4s_1s_3 + 3s_2^2 = 2p^4 - 12p^2q + 18q^2,$$
$$S_3 = 3s_6 - 6s_1s_5 + 15s_2s_4 - 10s_3^2$$
$$= 2p^6 - 18p^4q - 12p^3r + 57p^2q^2 + 54pqr - 66q^3 - 81r^2,$$

et enfin

$$P = -S_1 = -2p^2 + 6q,$$
$$Q = -\frac{S_2 + PS_1}{2} = p^4 - 6p^2q + 9q^2,$$
$$R = -\frac{S_3 + PS_2 + QS_1}{3} = 4p^3r - p^2q^2 - 18pqr + 4q^3 + 27r^2.$$

On suivrait une marche toute semblable pour former l'équation aux sommes deux à deux des racines d'une équation quelconque donnée.

La méthode générale dont nous venons de faire une application s'applique avec le même succès, que V soit ou non une fonction entière des racines a, b, c, etc.; mais on peut facilement démontrer qu'une fonction rationnelle d'une ou de plusieurs racines d'une équation peut toujours, si elle n'est pas entière, être remplacée par une fonction entière équivalente.

Sur la forme des fonctions rationnelles d'une ou de plusieurs racines d'une équation.

Nous commencerons par établir le théorème suivant, relatif aux fonctions rationnelles d'une seule racine.

THÉORÈME. — *Toute fonction rationnelle et non entière d'une racine a d'une équation*

$$(1) \qquad F(x) = 0$$

de degré m est équivalente à une fonction entière et de degré inférieur à m.

Soit, en effet, la fonction rationnelle $\frac{\varphi(a)}{\psi(a)}$, où φ et ψ désignent des fonctions entières; on aura identiquement

$$\frac{\varphi(a)}{\psi(a)} = \varphi(a) \cdot \frac{\psi(b)\psi(c)\ldots\psi(l)}{\psi(a)\psi(b)\ldots\psi(l)}, \tag{2}$$

$b, c, \ldots, l$ désignant les autres racines de l'équation (1). Or on voit que le dénominateur $\psi(a)\,\psi(b)\ldots\,\psi(l)$ du second membre est une fonction symétrique et entière des racines de l'équation (1), qui pourra, par conséquent, s'exprimer rationnellement par les coefficients de cette équation. Pareillement le facteur $\psi(b)\,\psi(c)\ldots\psi(l)$ du numérateur est une fonction symétrique et entière des racines de l'équation

$$\frac{F(x)}{x-a} = 0,$$

et il pourra s'exprimer sous forme rationnelle et entière, en fonction des coefficients de cette équation, c'est-à-dire en fonction de a et des coefficients de l'équation (1). D'après cela, l'égalité (2) prendra la forme

$$\frac{\varphi(a)}{\psi(a)} = \varphi(a) \cdot \theta(a),$$

où $\theta(a)$ désigne un polynôme entier et rationnel, par rapport à a. En effectuant le produit des polynômes φ et θ, notre fraction deviendra

$$\frac{\varphi(a)}{\psi(a)} = A_0 + A_1 a + A_2 a^2 + \ldots + A_\mu a^\mu;$$

et je dis qu'on peut supposer le degré μ inférieur à m. En effet, de l'équation $F(a) = 0$ on peut tirer la valeur de a^m qui sera exprimée par un polynôme de degré $m-1$; en

multipliant par a cette valeur de a^m, on aura a^{m+1}, qui sera exprimée par un polynôme du degré m, mais qu'on pourra abaisser au degré $m-1$, en remplaçant a^m par sa valeur trouvée précédemment. En continuant ainsi, on exprimera chaque puissance de a, à partir de la $m^{ième}$, par un polynôme de degré $m-1$, et, par suite, on pourra chasser de l'expression de $\frac{\varphi(a)}{\psi(a)}$ que nous avons trouvée, toutes les puissances de a supérieures à la $(m-1)^{ième}$. Mais on peut aussi opérer comme il suit : Si μ est $> m$, on divisera le polynôme $A_0 + A_1 a + \ldots$ par $F(a)$, et en désignant par Q le quotient, par $\varpi(a)$ le reste qui est de degré inférieur à m, on aura

$$\frac{\varphi(a)}{\psi(a)} = A_0 + A_1 a + \ldots = F(a) \times Q + \varpi(a);$$

et comme $F(a)$ est nul, on aura simplement

$$\frac{\varphi(a)}{\psi(a)} = \varpi(a),$$

où ϖ désigne un polynôme de degré $m-1$ au plus.

Quoique la démonstration précédente ne laisse rien à désirer sous le rapport de la rigueur et de la clarté, nous en donnerons une seconde qui aura l'avantage de nous fournir un procédé plus facile pour trouver la forme entière qui convient à une fonction fractionnaire donnée.

Soit toujours $\frac{\varphi(a)}{\psi(a)}$ la fraction donnée, où a est racine de $F(x) = 0$. On peut supposer $\psi(a)$ de degré inférieur à m, car si le contraire avait lieu, on ferait disparaître de $\psi(a)$ les puissances de a supérieures à la $(m-1)^{ième}$ par l'un des procédés indiqués précédemment.

Cela posé, opérons sur les polynômes $F(a)$ et $\psi(a)$, comme s'il était question de trouver leur plus grand com-

mun diviseur ; on aura cette suite d'égalités :

$$F(a) = \psi(a)\,Q_1 + R_1,$$
$$\psi(a) = R_1 Q_2 + R_2,$$
$$R_1 = R_2 Q_3 + R_3,$$
$$\cdots\cdots\cdots\cdots$$
$$R_{n-2} = R_{n-1} Q_n + R_n,$$

où R_n ne contient plus la quantité a. Or, $F(a)$ étant nul, on aura

$$R_1 = -Q_1\,\psi(a),$$
$$R_2 = (1 + Q_1 Q_2)\,\psi(a),$$
$$R_3 = -(Q_1 + Q_3 + Q_1 Q_2 Q_3)\,\psi(a),$$
$$\cdots\cdots\cdots\cdots$$

La dernière de ces égalités sera de la forme

$$R_n = \theta(a).\psi(a),$$

$\theta(a)$ désignant un polynôme entier et rationnel par rapport à a. On en tire

$$\psi(a) = \frac{R_n}{\theta(a)},$$

et, par suite,

$$\frac{\varphi(a)}{\psi(a)} = \frac{\varphi(a).\theta(a)}{R_n}.$$

Cette valeur de $\frac{\varphi(a)}{\psi(a)}$ est entière par rapport à a, puisque R_n ne contient pas a ; et, si elle renferme des puissances de a supérieures à la $(m-1)^{ième}$, on pourra les faire disparaître par le procédé que nous avons indiqué précédemment.

A la vérité, cette méthode semble en défaut dans le cas où les polynômes $\psi(x)$ et $F(x)$ ont un diviseur commun ; car, dans ce cas, la quantité désignée par R_n est nulle, ainsi que $\theta(a)$: mais alors on pourra enlever de $F(x)$, par une simple division, tous les facteurs linéaires qui sont dans $\psi(x)$, et parmi lesquels ne se trouve pas $x-a$, car autrement $\psi(a)$ serait nul. En désignant par $F_1(x)$

le résultat ainsi obtenu, a sera racine de $F_1(x) = 0$, et le polynôme $\psi(x)$ étant dès lors premier avec $F_1(x)$, on pourra appliquer la méthode précédente.

Corollaire. — La fonction rationnelle la plus générale d'une racine d'une équation de degré m est une fonction entière du degré $m - 1$, renfermant par conséquent m coefficients arbitraires.

Extension aux fonctions rationnelles de plusieurs racines d'une équation. — La méthode précédente a surtout l'avantage de pouvoir être appliquée aux fonctions rationnelles de plusieurs racines d'une équation. On a, en effet, ce théorème :

Toute fonction rationnelle non entière de plusieurs racines d'une équation peut être remplacée par une fonction entière des mêmes racines.

Rien ne sera changé à nos raisonnements, si la fonction $\frac{\varphi(a)}{\psi(a)}$, que nous avons considérée, renferme d'autres racines b, c, etc., de l'équation $F(x) = 0$, et cette fonction pourra se mettre sous la forme $A_0 a + A_1 a^2 + \dots$, A_0 et A_1 étant des fonctions rationnelles de racines parmi lesquelle ne se trouve pas a. A leur tour, on pourra rendre ces fonctions A_0, A_1, etc., entières par rapport à une autre racine b, puis par rapport à une troisième, et ainsi de suite.

Exemple. — Toute fonction rationnelle d'une racine a de l'équation du troisième degré

$$x^3 + px^2 + qx + r = 0$$

peut être mise sous la forme

$$A + Ba + Ca^2;$$

mais il est souvent préférable de prendre une forme fractionnaire dont les deux termes soient linéaires, et cela est toujours possible; car si l'on divise les polynômes

$a^3 + pa^2 + qa + r$ et $Ca^2 + Ba + A$, dont le premier est nul, l'un par l'autre, on aura un quotient et un reste du premier degré en a, et l'on conclut aisément de là que la fonction $A + Ba + Ca^2$ peut être mise sous la forme $\frac{Ma + N}{a + P}$.

Méthode d'élimination fondée sur la théorie des fonctions symétriques.

Parmi les applications que l'on peut faire de la théorie des fonctions symétriques, l'une des plus importantes est, sans contredit, la méthode d'élimination que nous allons expliquer.

Considérons deux équations, des degrés m et n respectivement, contenant deux ou un plus grand nombre de variables x, y, etc., et entre lesquelles il s'agit d'éliminer x. Nous supposerons ces équations complètes, et leurs coefficients entièrement indéterminés, et les ordonnant par rapport à x, nous les représenterons par

$$(1) \qquad x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

$$(2) \qquad x^n + q_1 x^{n-1} + q_2 x^{n-2} + \ldots + q_{n-1} x + q_n = 0.$$

Les coefficients p_1, p_2, etc., q_1, q_2, etc., sont des fonctions entières de y, etc.

Désignons par a, b, c,..., k, l les m racines de la première de ces deux équations, lesquelles dépendent de y et des autres variables, s'il y en a, et portons-les dans la seconde équation ; on aura ces m résultats

$$(3) \qquad \left\{ \begin{array}{l} a^n + q_1 a^{n-1} + q_2 a^{n-2} + \ldots + q_{n-1} a + q_n, \\ b^n + q_1 b^{n-1} + q_2 b^{n-2} + \ldots + q_{n-1} b + q_n, \\ c^n + q_1 c^{n-1} + q_2 c^{n-2} + \ldots + q_{n-1} c + q_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ l^n + q_1 l^{n-1} + q_2 l^{n-2} + \ldots + q_{n-1} l + q_n. \end{array} \right.$$

Cela posé, si l'on multiplie ensemble tous ces résultats, et que l'on désigne par V leur produit, il est facile de voir que

$$V = 0$$

sera l'équation finale résultant de l'élimination de x entre les deux équations proposées. En effet, l'équation finale qui résulte de l'élimination de x entre deux équations est simplement la condition nécessaire pour que ces deux équations aient une racine commune, et il est bien évident que la condition nécessaire et suffisante pour que les équations (1) et (2) aient une racine commune, est que l'un des résultats (3), ou leur produit V, soit nul.

D'ailleurs, V est une fonction symétrique et entière des racines de l'équation (1), qui contient, en outre, rationnellement les coefficients de l'équation (2); on pourra donc exprimer cette fonction rationnellement par les coefficients des équations (1) et (2).

En appliquant la méthode précédente à deux équations, dont les coefficients ont des valeurs particulières, on obtient toujours la véritable équation finale, pourvu que ces équations contiennent la plus haute puissance de l'inconnue qu'on élimine (*voir* la Note VI pour le cas des équations incomplètes). Cette méthode a, en outre, l'avantage de conduire à un théorème important, dont nous allons présenter la démonstration.

Théorème sur le degré de l'équation finale, qui résulte de l'élimination d'une inconnue entre deux équations.

Nous conserverons les notations employées dans le précédent paragraphe, et nous supposerons toujours que les deux équations (1) et (2), l'une du degré m, l'autre du degré n, soient complètes, et que leurs coefficients, représentés chacun par une lettre, soient dans une parfaite indépendance. Alors les quantités p_1 et q_1 sont des fonc-

tions entières du premier degré par rapport aux variables y, etc., qui entrent dans les équations proposées; pareillement, p_2, q_2 sont du deuxième degré, et, en général, le degré des coefficients de x dans les équations (1) et (2) sera indiqué par leur indice. Cela posé, nous allons démontrer le théorème suivant :

Le degré de l'équation finale qui résulte de l'élimination d'une variable x entre deux équations complètes dont les coefficients sont indéterminés et indépendants les uns des autres, est précisément égal au produit des degrés des deux équations.

Considérons, en effet, un terme quelconque du produit des expressions (3), par exemple

$$q_{n-\alpha}\, q_{n-6} \ldots q_{n-\lambda}\, a^{\alpha} b^{6} \ldots l^{\lambda};$$

ce terme se trouvera dans V, ainsi que la fonction symétrique dont il fait partie. V est donc la somme d'expressions de la forme

$$q_{n-\alpha}\, q_{n-6} \ldots q_{n-\lambda} \sum a^{\alpha} b^{6} \ldots l^{\lambda},$$

en observant qu'il faut remplacer $q_{n-\alpha}$ par 1, si $\alpha = n$, et de même pour les autres. Or, d'après ce qui a été dit plus haut, le facteur $q_{n-\alpha}\, q_{n-6} \ldots q_{n-\lambda}$ est du degré $(n-\alpha)+(n-6)+\ldots+(n-\lambda)$ ou $mn-(\alpha+6+\ldots+\lambda)$ par rapport aux variables y, etc.; si donc nous faisons voir que le second facteur $\sum a^{\alpha} b^{6} \ldots l^{\lambda}$ est, par rapport à ces mêmes variables y, etc., du degré $\alpha+6+\ldots+\lambda$, il s'ensuivra que le terme de V que nous considérons est du degré mn, et que V est lui-même de ce degré. Les coefficients p_1, p_2, etc., de l'équation (1) étant, par rapport à y, etc., d'un degré égal à leur indice, il en sera de même des sommes de puissances semblables s_1, s_2, etc., de ses racines; cela résulte immédiatement des formules

de Newton. Ainsi, le degré d'une fonction symétrique simple telle que s_α est le même, soit que l'on considère s_α comme fonction de a, b, etc., soit qu'on la considère comme fonction de y, etc. Enfin, $\sum a^\alpha b^6 \ldots l^\lambda$ peut s'exprimer en fonction des sommes s_α par une formule entière qui est du degré $\alpha + 6 + \ldots + \lambda$ par rapport aux racines a, b, etc., et qui est, par conséquent, aussi du même degré par rapport à y, etc. Le théorème est donc démontré.

Nous avons admis comme évident que les termes de degré mn, qui se trouvent dans V, ne peuvent se détruire, tant qu'on laisse indéterminés les coefficients des équations (1) et (2). Voici, au surplus, un moyen très-simple de le démontrer.

Considérons les deux équations

$$(1') \quad (x + a_1 y + b_1)(x + a_2 y + b_2)\ldots(x + a_m y + b_m) = 0,$$
$$(2') \quad (x + c_1 y + d_1)(x + c_2 y + d_2)\ldots(x + c_n y + d_n) = 0,$$

entre les deux inconnues x et y, et qui ont pour premiers membres, l'une (1') un produit de m facteurs linéaires, l'autre (2') un produit de n facteurs pareillement linéaires.

L'équation finale résultant de l'élimination de x entre les deux équations (1') et (2') aura évidemment pour premier membre le produit des mn facteurs linéaires dont l'expression générale est

$$(a_\mu - c_\nu)\, y + (b_\mu - d_\nu),$$

μ et ν pouvant prendre toutes les valeurs de 1 à m et de 1 à n respectivement; et si on laisse indéterminées les quantités a_1, b_1, c_1, d_1, etc., cette équation finale sera du degré mn.

D'ailleurs, cette équation finale doit être comprise dans l'équation V = 0, qui est relative aux équations gé-

nérales (1) et (2); donc cette dernière ne saurait être d'un degré inférieur à mn, à moins qu'on ne suppose aux coefficients des valeurs particulières.

Si les coefficients des équations (1) et (2) ont des valeurs déterminées, on pourra toujours appliquer le raisonnement qui précède, pourvu que ces équations contiennent la plus haute puissance de l'inconnue qu'on élimine. On est alors conduit à la proposition suivante, qui est générale :

Le degré de l'équation finale résultant de l'élimination d'une inconnue entre deux équations qui en contiennent plusieurs, est au plus égal au produit des degrés de ces équations.

Ce théorème a lieu encore si les équations que l'on considère manquent de la plus haute puissance de l'inconnue qu'on élimine.

Soient, en effet, deux équations entre deux variables x et y, ayant respectivement m et n pour degrés et manquant du terme le plus élevé en x. En considérant x et y comme des coordonnées rectilignes, ces deux équations appartiendront à deux courbes, et le degré de l'équation finale résultant de l'élimination de y sera égal au nombre des points d'intersection réels ou imaginaires de ces courbes. Par conséquent, ce nombre ne changera évidemment pas, si l'on rapporte les deux courbes à d'autres axes de coordonnées; mais alors les nouvelles équations de ces deux courbes se déduisent des anciennes, en remplaçant x et y par des fonctions linéaires $ax + by$, $a'x + b'y$, et contiendront évidemment, l'une un terme en x^m, l'autre un terme en x^n, à cause de l'indétermination de a et a'; le degré de l'équation finale en y résultant de l'élimination de x entre ces nouvelles équations sera donc au plus égal à mn : par suite, le nombre des points d'intersection des deux courbes ne pourra surpasser mn, et il en

sera de même du degré de l'équation finale qui résulterait de l'élimination de y entre les deux proposées.

La même démonstration s'applique au cas où les deux équations proposées contiennent, outre x et y, d'autres variables u, z,.... En effet, si l'on pose

$$z = ky, \quad u = k'y, \ldots,$$

et que l'on considère k, k', etc., comme des paramètres, le raisonnement précédent s'appliquera aux deux équations proposées qui ne renferment plus que x et y. Par où l'on voit que l'équation finale en y, z, u, etc., résultant de l'élimination de x, sera au plus du degré mn, si l'on y remplace z, u, etc., par ky, $k'y$, etc., et cela, quels que soient k, k', etc.; mais cette substitution ne change évidemment pas son degré, lequel ne pourra donc, en aucun cas, surpasser mn.

On peut au reste, dans chaque cas particulier, fixer avec précision le degré de l'équation finale qui résulterait de l'élimination d'une inconnue entre deux équations données. On trouvera dans la Note VI une règle très-simple pour résoudre cette question.

La méthode d'élimination par les fonctions symétriques, telle que nous l'avons exposée, ne donne pas le moyen de déterminer, dans la résolution de deux équations simultanées, la valeur de la seconde inconnue, qu'il faut joindre à chaque racine de l'équation finale. M. Liouville a cherché à combler cette lacune, et il y est parvenu (tome XII du *Journal de Mathématiques pures et appliquées*), comme nous l'indiquerons dans la leçon suivante.

QUATRIÈME LEÇON.

Méthode de M. Liouville pour la résolution de deux équations à deux inconnues. — Extension au cas d'un nombre quelconque d'équations entre un même nombre d'inconnues. — Méthode d'Abel pour déterminer la racine commune à deux équations. — Théorème de Lagrange sur les conditions nécessaires pour que deux équations aient plusieurs racines communes.

Méthode de M. Liouville pour la résolution de deux équations à deux inconnues.

Soient deux équations

(1) $$f(x, y) = 0, \quad F(x, y) = 0,$$

entre deux inconnues x et y; nous introduirons une autre variable t, telle que l'on ait

(2) $$t = x + \alpha y \quad \text{ou} \quad x = t - \alpha y,$$

α désignant un *paramètre* indéterminé. En mettant, au lieu de x, sa valeur $t - \alpha y$, les équations proposées deviennent

(3) $$f(t - \alpha y, y) = 0, \quad F(t - \alpha y, y) = 0.$$

Cela posé, nous éliminerons y entre les équations (3); nous obtiendrons ainsi une équation finale en t, renfermant le paramètre α, et nous la représenterons par

(4) $$\psi(t, \alpha) = 0;$$

comme pour $\alpha = 0$, on a $t = x$, l'équation finale en x qui résulterait de l'élimination de y entre les équations (1)

sera d'abord

(5) $$\psi(x, o) = o.$$

Voici maintenant comment on obtiendra la valeur de y qui correspond à chaque racine x de cette équation finale. Considérons t et α comme des coordonnées rectangulaires; l'équation (4) appartiendra à un lieu qui n'est autre chose qu'un système de droites réelles ou imaginaires, lesquelles seront aussi représentées par l'équation linéaire

$$t = x + \alpha y,$$

où l'on doit remplacer x et y successivement par les divers couples de solutions communes aux équations (1).

Considérons, en particulier, un couple de valeurs de x et y satisfaisant aux proposées, et la droite correspondante $t = x + \alpha y$, dont l'ordonnée à l'origine est $OM = x$ (*fig.* 1), et le coefficient angulaire tang $MAO = y$.

Supposons d'abord qu'à la valeur x que nous considérons ne corresponde qu'une seule valeur de y; la droite AB sera la seule des droites représentées par l'équation (4), qui passera par le point M : en d'autres termes, la droite AB sera la seule tangente au point M du lieu que représente l'équation (4). Mais le coefficient angulaire de la tangente en un point quelconque (t, α) de ce lieu s'obtient en différentiant l'équation (4); ce qui donne

(6) $$\frac{d\psi}{d\alpha} + \frac{d\psi}{dt}\frac{dt}{d\alpha} = o,$$

d'où

$$\frac{dt}{d\alpha} = -\frac{\frac{d\psi}{d\alpha}}{\frac{d\psi}{dt}} = \psi_1(t, \alpha),$$

équation qui ne sera en défaut que si l'on a en même

temps $\frac{d\psi}{d\alpha} = 0$, $\frac{d\psi}{dt} = 0$; ce qui n'a lieu que pour les points singuliers. Nous savons, d'ailleurs, qu'au point M, qui a pour coordonnées $\alpha = 0$ et $t = x$, la tangente a pour coefficient angulaire y; on a donc

$$y = \psi_1(x, 0),$$

et notre problème est résolu.

L'application de cette méthode exige un calcul plus long que si l'on se proposait seulement l'élimination de y entre les deux équations proposées; car le premier membre de l'équation finale (5) n'est que le premier terme de l'équation (4) ordonnée par rapport à α : mais on peut démontrer qu'il n'est pas nécessaire de calculer l'équation (4) tout entière, et qu'il suffit d'en connaître les deux premiers termes. Imaginons, en effet, que le polynôme $\psi(t, \alpha)$ soit ordonné par rapport aux puissances de α, de sorte que l'on ait

$$(7) \qquad \psi(t, \alpha) = \varpi(t) + \alpha\varpi_1(t) + \alpha^2\varpi_2(t) + \ldots,$$

et qu'on connaisse les deux premiers termes $\varpi(t)$ et $\varpi_1(t)$; l'équation finale en x sera d'abord

$$\varpi(x) = 0.$$

Ensuite on tire, en différentiant l'équation (7), et dénotant les dérivées à la manière de Lagrange,

$$(8) \qquad \begin{cases} \frac{d\psi}{dt} = \varpi'(t) + \alpha\varpi'_1(t) + \ldots, \\ \frac{d\psi}{d\alpha} = \varpi_1(t) + 2\alpha\varpi_2(t) + \ldots, \end{cases}$$

d'où

$$\psi_1(t, \alpha) = -\frac{\varpi_1(t) + 2\alpha\varpi_2(t) + \ldots}{\varpi'(t) + \alpha\varpi'_1(t) + \ldots},$$

et, par conséquent,

$$y = -\frac{\varpi_1(x)}{\varpi'(x)}.$$

L'équation précédente fera connaître la valeur de y qui correspond à chaque racine x, et elle ne sera en défaut que pour les valeurs de x auxquelles correspondent plusieurs valeurs de y. C'est le cas que nous allons actuellement examiner.

Supposons qu'à une même racine x de l'équation (5) correspondent deux valeurs de y que nous désignerons par y et y_1; alors les droites AB, A_1B_1 (*fig.* 2), représentées par les équations

$$t = x + \alpha y, \quad t = x + \alpha y_1,$$

passeront par un même point M de l'axe OT : autrement dit, au point M, qui est un point de la ligne représentée par l'équation (4), il y a deux tangentes à cette ligne, AB et A_1B_1; on a donc en ce point $\frac{d\psi}{d\alpha} = 0$, $\frac{d\psi}{dt} = 0$, et pour avoir la valeur de $\frac{dt}{d\alpha}$, il faut différentier l'équation (6), ce qui donne, à cause de $\frac{d\psi}{dt} = 0$,

$$(9) \qquad \frac{d^2\psi}{d\alpha^2} + 2\frac{d^2\psi}{d\alpha\, dt}\frac{dt}{d\alpha} + \frac{d^2\psi}{dt^2}\left(\frac{dt}{d\alpha}\right)^2 = 0.$$

En faisant $\alpha = 0$ et $t = x$, on tirera de cette équation deux valeurs de $\frac{dt}{d\alpha}$, qui seront précisément celles de y et y_1; et l'on peut voir aisément qu'il suffit de connaître les trois premiers termes de $\psi(t, \alpha)$. Différentions, en effet, les équations (8); on aura

$$\frac{d^2\psi}{dt^2} = \varpi''(t) + \alpha\varpi''_1(t) + \ldots,$$

$$\frac{d^2\psi}{d\alpha\, dt} = \varpi'_1(t) + 2\alpha\varpi'_2(t) + \ldots,$$

$$\frac{d^2\psi}{d\alpha^2} = 2\varpi_2(t) + \ldots.$$

D'après cela, faisant dans l'équation (9), $\alpha = 0$, $t = x$, $\frac{dt}{dx} = y$, on aura

$$\varpi''(x)\,y^2 + 2\varpi'_1(x)\,y + 2\varpi_2(x) = 0,$$

équation dont les racines sont les deux valeurs y et y_1, qui correspondent à x.

On voit, par là, comment il faudra opérer, si à une même valeur de x correspondent trois ou un plus grand nombre de valeurs de y. Je ne crois pas qu'il soit nécessaire d'insister davantage. Remarquons seulement que, pour qu'à une valeur de x correspondent deux valeurs de y, il faut que l'on ait en même temps

$$\varpi'(x) = 0, \quad \varpi_1(x) = 0;$$

pour qu'il y ait trois valeurs de y correspondantes à la valeur de x, il faut, de plus, que l'on ait

$$\varpi''(x) = 0, \quad \varpi'_1(x) = 0, \quad \varpi_2(x) = 0,$$

et ainsi de suite. Ces cas particuliers ne pourront donc jamais se présenter que si l'équation finale a des racines égales.

Extension au cas d'un nombre quelconque d'équations entre un même nombre d'inconnues.

La même méthode, où l'on peut éviter les considérations géométriques que j'ai cru devoir employer pour plus de clarté, s'applique au cas d'un nombre quelconque d'équations entre un pareil nombre d'inconnues.

Soient, par exemple, trois équations à trois inconnues x, y, z, savoir :

(1) $f(x, y, z) = 0$, $F(x, y, z) = 0$, $\varphi(x, y, z) = 0$;

on posera

(2) $t = x + \alpha y + 6 z$,

en désignant par t une nouvelle variable, et par α, 6 deux

indéterminées, puis on portera dans les équations (1) la valeur de x, tirée de l'équation (2) : on aura ainsi trois équations,

$$(3) \begin{cases} f(t-\alpha y-6z, y, z)=0, \quad F(t-\alpha y-6z, y, z)=0, \\ \varphi(t-\alpha y-6z, y, z)=0, \end{cases}$$

entre lesquelles on éliminera y et z (*). Soit

$$(4) \qquad \psi(t, \alpha, 6)=0$$

l'equation finale en t ainsi obtenue; on aura d'abord l'équation finale résultant de l'élimination de y et z entre les proposées, en faisant $t=x$, $\alpha=0$, $6=0$; ce sera donc

$$(5) \qquad \psi(x, 0, 0)=0.$$

Maintenant, pour avoir les valeurs y et z qui correspondent à chaque racine x de cette équation finale, on différentiera l'équation (4) par rapport à α, puis par rapport à 6; on obtiendra ainsi

$$(6) \begin{cases} \dfrac{dt}{d\alpha}=-\dfrac{\frac{d\psi}{d\alpha}}{\frac{d\psi}{dt}}=\psi_1(t, \alpha, 6), \\ \dfrac{dt}{d6}=-\dfrac{\frac{d\psi}{d6}}{\frac{d\psi}{dt}}=\psi_2(t, \alpha, 6). \end{cases}$$

D'ailleurs, en différentiant l'équation (2), on a

$$\frac{dt}{d\alpha}=y, \quad \frac{dt}{d6}=z;$$

faisant donc dans les équations (6) $\alpha=0$, $6=0$, $t=x$,

(*) La méthode d'élimination par les fonctions symétriques sera étendue, dans la huitième leçon, au cas d'un nombre quelconque d'équations.

on aura

$$y = \psi_1(x, 0, 0), \quad z = \psi_2(x, 0, 0).$$

Comme dans le cas de deux équations, il ne sera pas nécessaire de connaître les termes de $\psi(t, \alpha, 6)$ qui dépassent le premier degré en α et 6; car, si l'on suppose

$$\psi(t, \alpha, 6) = \varpi(t) + \alpha\varpi_1(t) + 6\varpi_2(t) + \ldots,$$

on aura

$$\frac{d\psi}{d\alpha} = \varpi_1(t) + \ldots,$$

$$\frac{d\psi}{d6} = \varpi_2(t) + \ldots,$$

$$\frac{d\psi}{dt} = \varpi'(t) + \ldots;$$

par conséquent, l'équation finale en x sera

$$\varpi(x) = 0,$$

et les valeurs de y et z seront

$$y = -\frac{\varpi_1(x)}{\varpi'(x)}, \quad z = -\frac{\varpi_2(x)}{\varpi'(x)}.$$

Si à une même valeur x correspondaient deux valeurs de y et de z, les formules précédentes seraient en défaut; il faudrait alors opérer comme nous l'avons fait dans le cas de deux équations. Ces cas d'exception n'offrent aucune difficulté, et je ne crois pas nécessaire de nous y arrêter davantage.

Au lieu d'employer deux indéterminées α et 6, comme nous l'avons fait, on peut se borner à une seule, et poser

(7) $$t = x + \alpha y + \alpha^2 z;$$

on remplacera dans les équations proposées x par $t - \alpha y - \alpha^2 z$ et on éliminera ensuite y et z; on obtiendra ainsi une équation finale

(8) $$\psi(t, \alpha) = 0.$$

L'équation finale en x s'en déduira, comme précédemment, en faisant $\alpha = 0$, $t = x$; cette équation sera donc

$$\psi(x, 0) = 0.$$

Pour avoir y et z, on différentiera deux fois l'équation (7), par rapport à α; ce qui donnera

$$\frac{dt}{d\alpha} = y + 2\alpha z, \quad \frac{d^2 t}{d\alpha^2} = 2z.$$

Cela posé, en différentiant l'équation (8), on trouve

$$(9) \qquad \frac{dt}{d\alpha} = -\frac{\frac{d\psi}{d\alpha}}{\frac{d\psi}{dt}} = \psi_1(t, \alpha),$$

d'où

$$(10) \qquad y + 2\alpha z = \psi_1(t, \alpha);$$

différentiant aussi cette équation (10) par rapport à α, on aura

$$2z = \frac{d\psi_1}{d\alpha} + \frac{d\psi_1}{dt}\frac{dt}{d\alpha},$$

ou, en remplaçant $\frac{dt}{d\alpha}$ par sa valeur tirée de l'équation (9),

$$(11) \qquad 2z = \frac{d\psi_1}{d\alpha} + \psi_1 \frac{d\psi_1}{dt} = \psi_2(t, \alpha).$$

Enfin, faisant $\alpha = 0$, $t = x$, dans les équations (10) et (11), on aura

$$y = \psi_1(x, 0), \quad 2z = \psi_2(x, 0).$$

Il est facile de voir qu'il n'est pas nécessaire de calculer l'équation (8) entièrement, et qu'il suffit d'en connaître les trois premiers termes.

Le problème dont nous venons de donner la solution, d'après M. Liouville, est compris, du moins lorsqu'il ne

s'agit que de deux équations, dans un autre problème plus général traité par Abel. Supposons qu'on ait deux équations

$$f(x, y) = 0, \quad F(x, y) = 0,$$

et qu'ayant éliminé y, on ait trouvé cette équation finale

$$\varpi(x) = 0,$$

cette dernière exprimant la condition pour que les deux proposées où y sera alors l'inconnue aient une racine commune, la recherche de la valeur de y, qui correspond à une racine de l'équation finale en x, est ramenée à trouver la racine commune y aux deux équations proposées. C'est précisément la question qu'Abel a résolue dans un Mémoire publié dans les *Annales de Mathématiques* de Gergonne, tome XVII, et qui ne fait pas partie du Recueil de ses œuvres complètes. Nous allons exposer sommairement l'analyse de ce grand géomètre.

Méthode d'Abel pour déterminer la racine commune à deux équations.

Quand deux équations ont une racine commune, on peut déterminer cette racine par la méthode du plus grand commun diviseur; mais on peut aussi, comme Abel l'a fait voir, former immédiatement l'expression de cette racine commune par la méthode des fonctions symétriques : on peut encore, par le même procédé, déterminer une fonction rationnelle quelconque de cette racine commune.

Soient les deux équations

$$(1)\quad f(y) = y^m + p_1 y^{m-1} + p_2 y^{m-2} + \ldots + p_{m-1} y + p_m = 0,$$
$$(2)\quad F(y) = y^n + q_1 y^{n-1} + q_2 y^{n-2} + \ldots + q_{n-1} y + q_n = 0,$$

qui ont une racine commune y_1, mais qui n'ont que cette

seule racine commune, et proposons-nous de calculer une fonction rationnelle et entière $\varphi(y_1)$ de cette racine.

Désignons par $y_1, y_2, \ldots, y_n$ les n racines de l'équation (2), et portons-les dans le premier membre de l'équation (1) $f(y)$; on aura ces n résultats

$$f(y_1),\quad f(y_2),\quad f(y_3),\ldots,\quad f(y_n),$$

dont le premier est nul. Faisons ensuite les produits $n-1$ à $n-1$ de ces n quantités, et désignons généralement par R_μ celui de ces produits qui ne contient pas le facteur $f(y_\mu)$; les quantités

$$R_1,\quad R_2,\quad R_3,\ldots,\quad R_n,$$

seront toutes nulles, à l'exception de la première. Cela posé, on aura identiquement

$$\begin{aligned} R_1\varphi(y_1) &= R_1\varphi(y_1) + R_2\varphi(y_2) + R_3\varphi(y_3) + \ldots + R_n\varphi(y_n) \\ &= \sum R\varphi(y), \end{aligned}$$

$$R_1 = R_1 + R_2 + R_3 + \ldots + R_n = \sum R,$$

d'où, par la division,

$$\varphi(y_1) = \frac{\Sigma R\varphi(y)}{\Sigma R},$$

le signe $\sum$ s'étendant à toutes les racines de l'équation (2). On voit que cette expression de $\varphi(y_1)$ est une fonction symétrique et rationnelle de toutes les racines de l'équation (2), et, par conséquent, on pourra la calculer par l'une des méthodes que nous avons exposées.

Tel est le principe de la méthode d'Abel; mais on peut, par un artifice ingénieux qu'il a indiqué, simplifier notablement le calcul de la fonction $\varphi(y_1)$. Soit $\theta(y)$ une fonction rationnelle quelconque dont nous nous réservons de déterminer ultérieurement la forme; on aura, de

même que précédemment,

$$R_1\theta(y_1)\varphi(y_1) = R_1\theta(y_1)\varphi(y_1) + R_2\theta(y_2)\varphi(y_2) + \ldots$$
$$+ R_n\theta(y_n)\varphi(y_n) = \sum R\theta(y)\varphi(y),$$
$$R_1\theta(y_1) = R_1\theta(y_1) + R_2\theta(y_2) + \ldots + R_n\theta(y_n)$$
$$= \sum R\theta(y),$$

d'où, par la division,

$$\varphi(y_1) = \frac{\Sigma R\theta(y)\varphi(y)}{\Sigma R\theta(y)}.$$

Cette nouvelle expression de $\varphi(y_1)$ est, comme la précédente, une fonction symétrique des racines de l'équation (2) et pourra être calculée de la même manière; mais elle devient plus simple, comme on va le voir, en disposant convenablement de la fonction indéterminée $\theta(y)$. Nous désignerons par $F'(y)$ la dérivée de $F(y)$, et nous poserons avec Abel,

$$\theta(y) = \frac{1}{F'(y)};$$

la valeur de $\varphi(y_1)$ sera alors

$$\varphi(y_1) = \frac{\sum \frac{R\varphi(y)}{F'(y)}}{\sum \frac{R}{F'(y)}}.$$

Cela posé, les quantités $R_1, R_2, \ldots, R_n$ peuvent s'exprimer rationnellement, la première en fonction de y_1, la seconde en fonction de y_2, etc., la dernière en fonction de y_n. En effet, R_μ est une fonction symétrique des quantités $y_1, y_2, \ldots, y_n$, excepté y_μ, c'est-à-dire une fonction symétrique des racines de l'équation

$$\frac{F(y)}{y - y_\mu} = 0,$$

ou

$$\begin{array}{c|c|l} y^{n-1} + q_1 & y^{n-2} + q_2 & y^{n-3} + \ldots = 0. \\ + y_\mu & + q_1 y_\mu & \\ & + y_\mu^2 & \end{array}$$

R_μ pourra donc s'exprimer sous forme rationnelle et entière en fonction de y_μ et des quantités connues qui entrent dans les équations (1) et (2), de la manière suivante :

$$R_\mu = \rho_0 + \rho_1 y_\mu + \rho_2 y_\mu^2 + \ldots + \rho_p y_\mu^p.$$

En outre, par l'un des procédés indiqués dans la troisième leçon, on pourra chasser de l'expression de R_μ toutes les puissances de y_μ supérieures à la $(n-1)^{ième}$, en sorte que la valeur de R_μ aura finalement cette forme :

$$(3) \qquad R_\mu = \rho_0 + \rho_1 y_\mu + \rho_2 y_\mu^2 + \ldots + \rho_{n-1} y_\mu^{n-1};$$

et l'on déduira de cette équation les valeurs de R_1, $R_2, \ldots, R_\mu$, en donnant successivement à l'indice μ les valeurs $1, 2, 3, \ldots, n$.

La quantité $R_\mu \varphi(y_\mu)$ pourra également s'exprimer par un polynôme entier et rationnel par rapport à y_μ de degré $n-1$, et qu'on calculera aisément quand R_μ sera trouvé : soit donc

$$R_\mu \varphi(y_\mu) = t_0 + t_1 y_\mu + t_2 y_\mu^2 + \ldots + t_{n-1} y_\mu^{n-1}.$$

Mais par un théorème connu (*), si $\psi(y)$ désigne un polynôme quelconque du degré $n-1$, la somme

$$\sum \frac{\psi(y)}{F'(y)},$$

(*) Ce théorème, qui résulte de la théorie de la décomposition d'une fraction rationnelle en fractions simples, sera démontré dans la leçon suivante.

étendue aux racines $y_1, y_2, \ldots, y_n$ de l'équation

$$F(y) = 0,$$

a pour valeur le coefficient de y^{n-1} dans $\psi(y)$; on aura, d'après cela,

$$\sum \frac{R\varphi(y)}{F'(y)} = t_{n-1},$$

$$\sum \frac{R}{F'(y)} = \rho_{n-1},$$

et, par suite,

$$(4) \qquad \varphi(y_1) = \frac{t_{n-1}}{\rho_{n-1}}.$$

Il suffit donc, pour avoir la valeur de notre fonction entière $\varphi(y_1)$, de calculer les coefficients de y^{n-1} dans R_μ et $R_\mu \varphi(y_\mu)$. Pour une autre fonction entière $\Phi(y_1)$, on aurait pareillement

$$\Phi(y_1) = \frac{T_{n-1}}{\rho_{n-1}},$$

T_{n-1} désignant le coefficient de y_μ^{n-1} dans $R_\mu \Phi(y_\mu)$; et, par suite, pour une fonction rationnelle $\frac{\Phi(y_1)}{\varphi(y_1)}$, on aura

$$\frac{\Phi(y_1)}{\varphi(y_1)} = \frac{T_{n-1}}{t_{n-1}}.$$

Si l'on veut seulement calculer y_1, il faudra faire $\varphi(y_1) = y_1$ dans l'équation (4); t_{n-1} sera alors le coefficient de y_μ^{n-1} dans $R_\mu y_\mu$: or, en multipliant l'équation (3) par y_μ, on trouve

$$R_\mu y_\mu = \rho_0 y_\mu + \rho_1 y_\mu^2 + \ldots + \rho_{n-2} y_\mu^{n-1} + \rho_{n-1} y_\mu^n,$$

et, en chassant y_μ^n à l'aide de l'équation (2),

$$y_\mu^n + q\, y_\mu^{n-1} + q_2 y_\mu^{n-2} + \ldots + q_{n-1} y + q = 0,$$

on a

$$R_\mu y_\mu = \ldots + (\rho_{n-2} - q_1 \rho_{n-1}) y_\mu^{n-1},$$

et, par suite,

$$t_{n-1} = \rho_{n-2} - q_1 \rho_{n-1};$$

la valeur de y_1 sera donc

$$y_1 = \frac{\rho_{n-2} - q_1 \rho_{n-1}}{\rho_{n-1}} = \frac{\rho_{n-2}}{\rho_{n-1}} - q_1.$$

Par où l'on voit qu'il suffit, pour avoir y_1, de calculer dans R_μ les coefficients de y_μ^{n-1} et de y_μ^{n-2}.

C'est ici l'occasion de mentionner un beau théorème que Lagrange a démontré dans son célèbre Mémoire inséré parmi ceux de l'Académie de Berlin pour 1770 et 1771, et qui est relatif aux conditions nécessaires pour que deux équations aient plusieurs racines communes.

Théorème de Lagrange sur les conditions nécessaires pour que deux équations aient plusieurs racines communes.

L'objet de ce théorème est de faire connaître les conditions pour que deux équations algébriques aient deux, trois, etc., racines communes, quand on connaît la condition pour qu'elles en aient une. Voici en quoi il consiste.

Si $V = 0$ *exprime la condition pour que deux équations algébriques*

$$(1)\quad f(x) = x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$
$$(2)\quad F(x) = x^n + q_1 x^{n-1} + q_2 x^{n-2} + \ldots + q_{n-1} x + q_n = 0,$$

aient une racine commune, V *désignant une fonction entière des coefficients* $p_1, p_2, \ldots, q_1, q_2, \ldots$, *les condi-*

tions nécessaires pour deux racines communes seront

$$V = o \quad \text{et} \quad \frac{dV}{dp_m} = o,$$

ou bien

$$V = o \quad \text{et} \quad \frac{dV}{dq_n} = o;$$

pareillement les conditions nécessaires pour trois racines communes seront

$$V = o, \quad \frac{dV}{dp_m} = o, \quad \frac{d^2V}{dp_m^2} = o,$$

ou bien

$$V = o, \quad \frac{dV}{dq_n} = o, \quad \frac{d^2V}{dq_n^2} = o,$$

et ainsi de suite; en sorte qu'on obtiendra les conditions nécessaires pour μ racines communes, en joignant à l'équation nécessaire pour une seule racine commune les $\mu - 1$ équations qu'on en déduit en la différentiant $\mu - 1$ fois par rapport au dernier terme de l'une des deux équations proposées.

Tel est l'énoncé que Lagrange a donné de son théorème; mais il est nécessaire d'ajouter quelques mots sur la manière dont cet énoncé doit être entendu. Ainsi les équations

$$V = o, \quad \frac{dV}{dp_m} = o, \quad \frac{d^2V}{dp_m^2} = o, \ldots, \quad \frac{d^{\mu-1}V}{dp_m^{\mu-1}} = o,$$

expriment simplement les conditions nécessaires et suffisantes pour que μ racines de l'équation (2) satisfassent à l'équation (1), en sorte que si l'équation (2) a des racines égales, il sera possible de satisfaire aux μ équations de condition écrites plus haut, sans que les premiers membres des équations (1) et (2) aient un diviseur commun du degré μ, ce qui serait la condition nécessaire pour que les

équations (1) et (2) eussent réellement μ racines communes. Pareillement les équations

$$V=0, \quad \frac{dV}{dq_n}=0, \quad \frac{d^2V}{dq_n^2}=0, \ldots, \quad \frac{d^{\mu-1}V}{dq_n^{\mu-1}}=0,$$

expriment les conditions nécessaires pour que μ racines de l'équation (1) satisfassent à l'équation (2), en sorte que si l'équation (1) a des racines multiples, on pourra satisfaire aux équations de condition précédentes, sans que les équations (1) et (2) aient réellement μ racines communes.

Il faut remarquer, en outre, que le dernier terme p_m ou q_n, par rapport auquel sont prises les dérivées de V, doit être considéré comme un paramètre indéterminé dont tous les autres coefficients sont indépendants.

Cela posé, passons à la démonstration du théorème. Soient $a, b, c, \ldots k, l$ les n racines de l'équation (2), et posons

$$V=f(a)f(b)\ldots f(k)f(l);$$

V est une fonction symétrique des racines de l'équation (2), dont les coefficients sont des fonctions entières des coefficients de l'équation (1); on pourra donc exprimer cette quantité par une fonction entière des coefficients des équations (1) et (2).

Les racines $a, b, c, \ldots, k, l$ étant indépendantes de p_m, les dérivées des quantités $f(a), f(b), \ldots, f(l)$ par rapport à p_m sont toutes égales à l'unité; donc $\frac{dV}{dp_m}$ est égale à la somme des produits $m-1$ à $m-1$ des quantités

$$f(a), \quad f(b), \ldots, \quad f(k), \quad f(l);$$

pareillement $\frac{1}{1.2}\frac{d^2V}{dp_m^2}$ est égale à la somme des produits $m-2$ à $m-2$ des mêmes quantités, et généralement

$\frac{1}{1.2\ldots i}\frac{d^iV}{dp_m^i}$ est égale à la somme de leurs produits $m-i$ à $m-i$.

Par conséquent, l'équation qui a pour racines les n quantités

$$f(a),\ f(b),\ \ldots,\ f(k),\ f(l)$$

est

$$X^n-\frac{1}{1.2\ldots(n-1)}\frac{d^{n-1}V}{dp_m^{n-1}}X^{n-1}+\ldots\mp\frac{1}{1.2.3}\frac{d^3V}{dp_m^3}X^3$$
$$\pm\frac{1}{1.2}\frac{d^2V}{dp_m^2}X^2\mp\frac{dV}{dp_m}X\pm V=0.$$

Or, pour que μ racines de l'équation (2) satisfassent à l'équation (1), il faut et il suffit que l'équation en X ait μ racines nulles, c'est-à-dire que l'on ait

$$V=0,\quad \frac{dV}{dp_m}=0,\quad \frac{d^2V}{dp^2}=0,\ldots,\quad \frac{d^{\mu-1}V}{dp_m^{\mu-1}}=0,$$

ce qui démontre le théorème énoncé.

La démonstration qui précède est plus claire et plus précise que celle qui a été donnée par Lagrange. Il semble effectivement au premier abord, par le raisonnement de l'auteur, qu'il est permis, dans l'énoncé du théorème, de substituer aux dérivées de V, prises par rapport au dernier terme de l'une des équations proposées, les dérivées prises par rapport à un coefficient quelconque, ou même par rapport à un paramètre dont un ou plusieurs de ces coefficients seraient fonctions. Mais il est aisé de voir qu'on obtiendrait de cette manière des équations de condition trop générales.

Par exemple, p_{m-i} étant le coefficient de x^i dans $f(x)$, et tous les autres coefficients étant indépendants de p_{m-i},

les équations

$$\mathrm{V} = 0, \quad \frac{d\mathrm{V}}{dp_{m-i}} = 0$$

peuvent avoir lieu, quoique les équations (1) et (2) n'aient qu'une seule racine commune. En effet, les dérivées de $f(a)$, $f(b)$,..., $f(l)$, par rapport à p_{m-i}, ont respectivement pour valeurs a^i, b^i,..., l^i; donc, à cause de

$$\mathrm{V} = f(a)f(b)\ldots f(l),$$

on aura

$$\frac{d\mathrm{V}}{dp_{m-i}} = a^i f(b)\ldots f(l) + b^i f(a)\ldots f(l) + \ldots$$

Il est évident, d'après cela, que les équations

$$\mathrm{V} = 0, \quad \frac{d\mathrm{V}}{dp_{m-i}} = 0$$

seront vérifiées si chacune des équations proposées a une racine nulle.

Exemple. — Appliquons le théorème de Lagrange aux deux équations

$$x^3 + p_1 x^2 + p_2 x + p_3 = 0,$$
$$x^2 + q_1 x + q_2 = 0.$$

En appelant a et b les racines de la seconde équation, on a

$$\begin{aligned}\mathrm{V} &= (a^3 + p_1 a^2 + p_2 a + p_3)(b^3 + p_1 b^2 + p_2 b + p_3)\\ &= q_2^3 - q_1 q_2^2 p_1 + (q_1^2 q_2 - 2q_2^2)p_2 - (q_1^3 - 3q_1 q_2)p_3 + q_2^2 p_1^2\\ &\quad - q_1 q_2 p_1 p_2 + (q_1^2 - 2q_2)p_1 p_3 + q_2 p_2^2 - q_1 p_2 p_3 + p_3^2,\end{aligned}$$

et

$$\frac{d\mathrm{V}}{dp_3} = -q_1^3 + 3q_1 q_2 + (q_1^2 - 2q_2)p_1 - q_1 p_2 + 2p_3.$$

La condition, pour que les proposées aient une racine commune, est $V = 0$; par suite, les conditions pour deux racines communes sont

$$V = 0, \qquad \frac{dV}{dp_3} = 0.$$

En éliminant p_3 entre celles-ci, il vient

$$(q_1^2 - 4q_2)(q_1^2 - q_2 - q_1p_1 + p_2)^2 = 0;$$

cette dernière se décompose en deux autres. En prenant

$$q_1^2 - 4q_2 = 0,$$

on exprime que les deux racines de l'équation du second degré sont égales entre elles, et ces racines satisfont à l'équation du troisième degré en vertu de la condition $V = 0$. En prenant, au contraire,

$$q_1^2 - q_2 - q_1p_1 + p_2 = 0,$$

l'équation $\frac{dV}{dp_3} = 0$ se réduit à

$$q_1q_2 - q_2p_1 + p_3 = 0.$$

Les deux équations précédentes expriment les conditions nécessaires et suffisantes pour que la première des équations proposées soit divisible par la seconde.



CINQUIÈME LEÇON.

Décomposition en fractions simples, d'une fraction rationnelle dont le dénominateur n'a pas de facteurs multiples. — Démonstration d'une formule d'analyse. — Méthode de M. Liouville pour décomposer une fraction rationnelle en fractions simples. — Cas des fractions rationnelles dont le dénominateur a des facteurs multiples.

Nous nous sommes appuyé, dans la dernière leçon, sur une formule que l'on peut déduire de la théorie de la décomposition des fractions rationnelles en fractions simples, ou qui, inversement, peut être prise pour le point de départ de cette théorie. Nous allons étudier en détail ce double point de vue. Nous commencerons par établir un procédé pour décomposer en fractions simples une fraction rationnelle dont le dénominateur n'a pas de facteurs multiples, et nous en déduirons la formule dont nous venons de parler. Nous donnerons ensuite, de cette même formule, une démonstration directe due à M. Liouville, et nous exposerons la méthode qu'il en a déduite pour former les fractions simples dans lesquelles peut se décomposer une fraction rationnelle. Nous ferons voir, enfin, comment on peut passer du cas des fractions rationnelles dont le dénominateur n'a que des facteurs simples, au cas des fractions dont le dénominateur a des facteurs multiples.

Décomposition en fractions simples, d'une fraction rationnelle dont le dénominateur n'a pas de facteurs multiples.

Théorème. — *Soient*

$$f(x) = (x-a)(x-b)(x-c)\ldots(x-l)$$

un polynôme du degré m dont toutes les racines a, b, c,..., l sont inégales, et F (x) *un polynôme du degré* $m-1$ *au plus; il y aura un système de valeurs des constantes* A, B, C,..., L, *tel que l'on aura identiquement*

$$(1)\quad \frac{F(x)}{f(x)} = \frac{A}{x-a} + \frac{B}{x-b} + \frac{C}{x-c} + \ldots + \frac{L}{x-l},$$

et il n'y en aura qu'un seul.

L'équation (1) peut s'écrire ainsi :

$$(2)\quad F(x) = \frac{Af(x)}{x-a} + \frac{Bf(x)}{x-b} + \ldots + \frac{Lf(x)}{x-l};$$

et si l'on admet qu'elle soit identique, elle sera satisfaite quand on donnera à x les valeurs a, b, c,..., l; mais pour $x=a$, tous les termes du second membre sont nuls, à l'exception du premier $A\frac{f(x)}{x-a}$ qui se réduit à $Af'(a)$: on a donc

$$F(a) = Af'(a),\quad \text{d'où}\quad A = \frac{F(a)}{f'(a)}.$$

L'équation (2), ou, ce qui est la même chose, l'équation (1) ne peut donc avoir lieu identiquement que si l'on a

$$(3)\quad A = \frac{F(a)}{f'(a)},\quad B = \frac{F(b)}{f'(b)},\ldots,\quad L = \frac{F(l)}{f'(l)};$$

ces valeurs de A, B, etc., sont les seules qui puissent remplir la condition demandée. Pour prouver qu'elles la remplissent en effet, remarquons qu'en les adoptant, l'équation (2) sera satisfaite pour les m valeurs a, b,..., l de x, et sera par conséquent identique, puisque son degré est $m-1$ au plus : d'ailleurs, les valeurs trouvées pour A, B, etc., sont finies, car les racines a, b, etc.,

sont inégales. On a donc la valeur suivante de la fraction rationnelle $\frac{F(x)}{f(x)}$:

$$\frac{F(x)}{f(x)} = \frac{F(a)}{f'(a)}\frac{1}{x-a} + \frac{F(b)}{f'(b)}\frac{1}{x-b} + \ldots + \frac{F(l)}{f'(l)}\frac{1}{x-l}.$$

Supposons maintenant que le numérateur de la fraction rationnelle $\frac{F(x)}{f(x)}$ soit d'un degré égal ou supérieur à celui du dénominateur. Désignons par $E(x)$ le quotient de la division de $F(x)$ par $f(x)$, et par $\varphi(x)$ le reste : on aura

$$\frac{F(x)}{f(x)} = E(x) + \frac{\varphi(x)}{f(x)} = E(x) + \frac{\varphi(a)}{f'(a)}\frac{1}{x-a} + \ldots + \frac{\varphi(l)}{f'(l)}\frac{1}{x-l};$$

mais, à cause de $F(x) = E(x).f(x) + \varphi(x)$, on a

$$\varphi(a) = F(a), \quad \varphi(b) = F(b), \ldots,$$

donc

$$\frac{F(x)}{f(x)} = E(x) + \frac{F(a)}{f'(a)}\frac{1}{x-a} + \frac{F(b)}{f'(b)}\frac{1}{x-b} + \ldots + \frac{F(l)}{f'(l)}\frac{1}{x-l}.$$

On voit que les fractions simples, dans lesquelles se décompose la fraction rationnelle, sont les mêmes que dans le premier cas; il faut seulement ajouter le quotient entier de la division du numérateur par le dénominateur.

Démonstration d'une formule d'analyse.

L'équation

$$F(x) = \frac{F(a)}{f'(a)}\frac{f(x)}{x-a} + \frac{F(b)}{f'(b)}\frac{f(x)}{x-b} + \ldots + \frac{F(l)}{f'(l)}\frac{f(x)}{x-l},$$

ayant lieu identiquement si F est de degré inférieur à f, les coefficients de x^{m-1} sont égaux dans les deux membres; si donc on désigne par P le coefficient de x^{m-1} dans $F(x)$.

on aura

$$P = \frac{F(a)}{f'(a)} + \frac{F(b)}{f'(b)} + \ldots + \frac{F(l)}{f'(l)},$$

ou

$$\sum \frac{F(x)}{f'(x)} = P.$$

Dans cette formule, $f'(x)$ désigne la dérivée d'un polynôme quelconque $f(x)$ de degré m, dont le premier terme a pour coefficient l'unité, et $F(x)$ est un polynôme quelconque de degré inférieur à m, dans lequel le coefficient de x^{m-1} est égal à P. Quant au signe $\sum$, il s'étend à toutes les racines de $f(x) = 0$. Cette formule est celle sur laquelle nous nous sommes appuyé dans la leçon précédente, et que nous avions admise sans la démontrer. Si le polynôme $F(x)$ est du degré $m - 2$ au plus, on aura $P = 0$, et, par suite,

$$\sum \frac{F(x)}{f'(x)} = 0.$$

Méthode de M. Liouville pour décomposer une fraction rationnelle en fractions simples.

M. Liouville a déduit de l'équation précédente un moyen ingénieux de présenter la théorie de la décomposition des fractions rationnelles (*). Nous allons exposer ici cette méthode.

Soient $f(x)$ et $F(x)$ deux polynômes des degrés m et $m - 1$ respectivement, ayant pour valeurs

$$f(x) = x^m + px^{m-1} + \ldots,$$
$$F(x) = Px^{m-1} + \ldots,$$

et considérons l'équation

$$(1) \qquad f(x) + \alpha F(x) = 0,$$

(*) *Journal de Mathématiques pures et appliquées*, tome XI, page 462.

où α désigne une indéterminée qui n'entre ni dans f, ni dans F; représentons par la notation $\sum x$ la somme des racines de l'équation (1), on aura

$$(2) \qquad \sum x = -p - \mathrm{P}\alpha,$$

et ces racines étant des fonctions de α, on aura, en différentiant l'équation (2) par rapport à α,

$$(3) \qquad \sum \frac{dx}{d\alpha} = -\mathrm{P}.$$

On a aussi, en différentiant l'équation (1) par rapport à α, et dénotant les dérivées à la manière ordinaire,

$$[f'(x) + \alpha \mathrm{F}'(x)] \frac{dx}{d\alpha} + \mathrm{F}(x) = 0;$$

d'où

$$\frac{dx}{d\alpha} = -\frac{\mathrm{F}(x)}{f'(x) + \alpha \mathrm{F}'(x)}.$$

On pourra donc écrire l'équation (3) de la manière suivante :

$$\sum \frac{\mathrm{F}(x)}{f'(x) + \alpha \mathrm{F}'(x)} = \mathrm{P}.$$

Dans cette équation, le signe $\sum$ s'étend à toutes les racines de l'équation (1), et l'on peut considérer α comme une quantité entièrement arbitraire; faisant donc $\alpha = 0$, on aura

$$\sum \frac{\mathrm{F}(x)}{f'(x)} = \mathrm{P},$$

le signe $\sum$ s'étendant alors aux racines de l'équation

$$f(x) = 0.$$

Si f étant toujours du degré m, F n'est que du degré $m-2$

au plus, P sera nul, et l'on aura

$$\sum \frac{F(x)}{f'(x)} = 0.$$

Voici, maintenant, comment M. Liouville déduit de cette dernière formule le théorème relatif à la décomposition des fractions rationnelles.

Soient $F(x)$ un polynôme du degré $m-1$ au plus, $f(x)$ un polynôme du degré m, tel que

$$f(x) = (x-a)(x-b)\ldots(x-l),$$

et posons

$$\varphi(x) = (x-t)f(x);$$

le degré du polynôme $\varphi(x)$ surpassant de deux unités au moins celui de $F(x)$, on aura, d'après le théorème qui vient d'être établi,

$$\sum \frac{F(x)}{\varphi'(x)} = 0,$$

ou, comme $a, b, c, \ldots, l$ et t sont les racines de $\varphi(x) = 0$,

$$(4) \qquad \frac{F(t)}{\varphi'(t)} + \frac{F(a)}{\varphi'(a)} + \frac{F(b)}{\varphi'(b)} + \ldots + \frac{F(l)}{\varphi'(l)} = 0.$$

Cela posé, en différentiant l'équation

$$\varphi(x) = (x-t)f(x),$$

on trouve

$$\varphi'(x) = (x-t)f'(x) + f(x);$$

on aura donc

$$\varphi'(t) = f(t)$$

et

$$\varphi'(a) = (a-t)f'(a), \quad \varphi'(b) = (b-t)f'(b), \ldots.$$

D'après cela, l'équation (4) donnera

$$\frac{F(t)}{f(t)} = \frac{F(a)}{f'(a)}\,\frac{1}{t-a} + \frac{F(b)}{f'(b)}\,\frac{1}{t-b} + \ldots + \frac{F(l)}{f'(l)}\,\frac{1}{t-l},$$

ce qui est précisément la formule à laquelle nous avons été conduit par la première méthode.

Cas des fractions rationnelles dont le dénominateur a des facteurs multiples.

Du cas d'une fraction rationnelle dont le dénominateur n'a que des facteurs simples, on peut passer à celui d'une fraction dont le dénominateur a des facteurs multiples, en employant un artifice qui nous a déjà servi dans une précédente leçon.

Supposons, par exemple, que parmi les m racines a, b, c,..., k, l de l'équation $f(x)=0$, deux soient égales entre elles, que l'on ait $b=a$, mais que toutes les autres racines soient inégales et différentes de a, et soit toujours $F(x)$ un polynôme de degré inférieur au degré de $f(x)$; il s'agit de décomposer la fraction $\frac{F(x)}{f(x)}$ en fractions simples. Nous prendrons d'abord, au lieu de $f(x)$, un polynôme $\varphi(x)$, qu'on déduira de $f(x)$ en remplaçant l'une des deux racines a par une racine peu différente $a+h$; nous poserons, en un mot,

$$\varphi(x)=\frac{f(x)(x-a-h)}{x-a},$$

et alors nous aurons cette valeur de la fraction $\frac{F(x)}{\varphi(x)}$,

$$\frac{F(x)}{\varphi(x)}=\frac{F(a)}{\varphi'(a)}\frac{1}{x-a}+\frac{F(a+h)}{\varphi'(a+h)}\frac{1}{x-a-h}+\ldots+\frac{F(l)}{\varphi'(l)}\frac{1}{x-l}.$$

On a d'ailleurs

$$\frac{1}{x-a-h}=\frac{1}{x-a}+\frac{h}{(x-a)^2}+\frac{h^2}{(x-a)^3}+\ldots;$$

donc

$$\frac{F(x)}{\varphi(x)} = \left[\frac{F(a)}{\varphi'(a)} + \frac{F(a+h)}{\varphi'(a+h)}\right]\frac{1}{x-a}$$
$$+ \frac{hF(a+h)}{\varphi'(a+h)}\left[\frac{1}{(x-a)^2} + \frac{h}{(x-a)^3} + \ldots\right]$$
$$+ \frac{F(c)}{\varphi'(c)}\frac{1}{x-c} + \ldots + \frac{F(l)}{\varphi'(l)}\frac{1}{x-l}.$$

Mais la dérivée $\varphi'(x)$ de $\varphi(x)$ a pour valeur

$$\varphi'(x) = \frac{f'(x)(x-a-h)}{x-a} + \frac{f(x)}{x-a} - \frac{f(x)(x-a-h)}{(x-a)^2};$$

d'où, en faisant successivement $x=a$, $x=a+h$, et se rappelant que $f(x)=0$ a deux racines égales à a,

$$\varphi'(a) = -\frac{hf''(a)}{2}, \quad \varphi'(a+h) = \frac{f(a+h)}{h};$$

on aura, d'après cela,

$$\frac{F(x)}{\varphi(x)} = \left[\frac{hF(a+h)}{f(a+h)} - \frac{2F(a)}{hf''(a)}\right]\frac{1}{x-a}$$
$$+ \frac{h^2F(a+h)}{f(a+h)}\left[\frac{1}{(x-a)^2} + \frac{h}{(x-a)^3} + \ldots\right]$$
$$+ \frac{F(c)}{\varphi'(c)}\frac{1}{x-c} + \ldots + \frac{F(l)}{\varphi'(l)}\frac{1}{x-l}.$$

Or

$$\frac{hF(a+h)}{f(a+h)} - \frac{2F(a)}{hf''(a)} = \frac{h^2f''(a)F(a+h) - 2F(a)f(a+h)}{hf''(a)f(a+h)};$$

en développant $F(a+h)$ et $f(a+h)$ par la formule de Taylor, et se rappelant que $f(a)$ et $f'(a)$ sont nulles, on trouve que le second membre se réduit à

$$\frac{\left[F'(a)f''(a) - \frac{F(a)f'''(a)}{3}\right] + \left[\frac{F''(a)f''(a)}{2} - \frac{F(a)f^{\text{IV}}(a)}{12}\right]h + \ldots}{\frac{f''^2(a)}{2} + \frac{f''(a)f'''(a)}{6}h + \ldots}$$

On aura donc, pour $h = 0$,

$$\lim \left[\frac{h\,F(a+h)}{f(a+h)} - \frac{2\,F(a)}{h f''(a)} \right] = \frac{6\,F'(a) f''(a) - 2\,F(a) f'''(a)}{3\,f''^2(a)};$$

on a aussi

$$\lim \frac{h^2 F(a+h)}{f(a+h)} = \lim \frac{h^2 [F(a) + h\,F'(a) + \ldots]}{h^2 \frac{f''(a)}{2} + h^3 \frac{f'''(a)}{2.3} + \ldots} = \frac{2\,F(a)}{f''(a)}.$$

Faisant donc $h = 0$, dans la valeur de $\frac{F(x)}{\varphi(x)}$ écrite plus haut, on aura la valeur suivante de $\frac{F(x)}{f(x)}$

$$\frac{F(x)}{f(x)} = \frac{6\,F'(a) f''(a) - 2\,F(a) f'''(a)}{3 f''^2(a)} \frac{1}{x-a} + \frac{2\,F(a)}{f''(a)} \frac{1}{(x-a)^2}$$
$$+ \frac{F(c)}{f'(c)} \frac{1}{x-c} + \ldots + \frac{F(l)}{f'(l)} \frac{1}{x-l}.$$

On voit aisément comment il faudrait opérer dans le cas où $f(x)$ aurait trois ou un plus grand nombre de racines égales à a. Mais nous n'insisterons pas davantage sur cette méthode, de laquelle il ne semble pas qu'on puisse déduire un procédé commode pour déterminer généralement l'expression algébrique des différents termes dans lesquels peut se décomposer une fraction rationnelle; il nous suffit d'avoir montré, par ce qui précède, que la formule relative au cas d'une fraction rationnelle $\frac{F(x)}{f(x)}$, dont le dénominateur $f(x)$ n'a pas de racines égales, n'est pas aussi particulière qu'on aurait pu le croire, et qu'elle renferme implicitement tous les cas.

SIXIÈME LEÇON.

Théorie générale de la décomposition des fractions rationnelles en fractions simples. — Théorèmes sur la possibilité de décomposer une fraction rationnelle. — Méthodes pour effectuer la décomposition d'une fraction rationnelle en fractions simples.

Théorie générale de la décomposition des fractions rationnelles en fractions simples.

Nous avons été conduit naturellement, par une question incidente, à nous occuper de la décomposition des fractions rationnelles en fractions simples. Les détails dans lesquels nous sommes entré à ce sujet, suffisent pour l'objet que nous avions en vue; mais la théorie des fractions rationnelles est si importante, et ses applications dans l'analyse mathématique si variées, que je crois utile de la reprendre ici, en lui donnant tous les développements qu'elle comporte.

Nous commencerons par établir qu'une fraction rationnelle $\frac{F(x)}{f(x)}$, dont les deux termes sont des polynômes quelconques premiers entre eux, est décomposable en une partie entière (qui peut être nulle), et en plusieurs *fractions simples* à numérateurs constants, ayant pour dénominateurs les diverses puissances des facteurs linéaires qui peuvent diviser le polynôme $f(x)$. Nous démontrerons ensuite qu'une fraction rationnelle n'est décomposable ainsi que d'une seule manière, et nous indiquerons enfin le moyen d'effectuer la décomposition.

Théorèmes sur la possibilité de décomposer une fraction rationnelle.

THÉORÈME I. — *Si a désigne une racine de l'équation $f(x)=0$, α son degré de multiplicité, en sorte que l'on ait*

$$f(x)=(x-a)^\alpha f_1(x),$$

$f_1(x)$ étant un polynôme non divisible par $x-a$, la fraction rationnelle $\frac{F(x)}{f(x)}$, supposée irréductible, pourra toujours être décomposée en deux parties de la manière suivante :

$$\frac{F(x)}{f(x)}=\frac{A}{(x-a)^\alpha}+\frac{F_1(x)}{(x-a)^{\alpha-1}f_1(x)},$$

A étant une constante, et $F_1(x)$ un polynôme entier et rationnel.

En effet, on a identiquement, et quel que soit A,

$$\frac{F(x)}{f(x)}=\frac{F(x)}{(x-a)^\alpha f_1(x)}=\frac{A}{(x-a)^\alpha}+\frac{F(x)-Af_1(x)}{(x-a)^\alpha f_1(x)},$$

et pour que le deuxième terme du second membre ne contienne à son dénominateur que la puissance $\alpha-1$ du facteur $x-a$, il faut et il suffit que le numérateur $F(x)-Af_1(x)$ s'annule pour $x=a$. Posons donc

$$F(a)-Af_1(a)=0, \quad \text{d'où} \quad A=\frac{F(a)}{f_1(a)};$$

cette valeur de A sera finie et différente de zéro, puisque $f_1(a)$ et $F(a)$ ne sont pas nuls : or, si l'on fait

$$F(x)-Af_1(x)=(x-a)F_1(x),$$

on aura

$$\frac{F(x)}{f(x)}=\frac{A}{(x-a)^\alpha}+\frac{F_1(x)}{(x-a)^{\alpha-1}f_1(x)};$$

ce qu'il fallait démontrer

Corollaire. — En appliquant le même théorème à la fraction $\frac{F_1(x)}{(x-a)^{\alpha-1}f_1(x)}$, on pourra la mettre sous la forme

$$\frac{A_1}{(x-a)^{\alpha-1}}+\frac{F_2(x)}{(x-a)^{\alpha-2}f_1(x)},$$

A_1 étant une constante et $F_2(x)$ une fonction entière; seulement ici A_1 peut être nulle, car $F_1(x)$ peut admettre le facteur $x-a$. En continuant ainsi, on voit que la fraction rationnelle $\frac{F(x)}{f(x)}$ peut être décomposée de la manière suivante :

$$\frac{F(x)}{f(x)}=\frac{F(x)}{(x-a)^{\alpha}f_1(x)}=\frac{A}{(x-a)^{\alpha}}+\frac{A_1}{(x-a)^{\alpha-1}}+\ldots$$
$$+\frac{A_{\alpha-1}}{x-a}+\frac{F_{\alpha}(x)}{f_1(x)},$$

A, A_1, A_2, etc., étant des constantes finies et déterminées dont la première n'est pas nulle, et $F_{\alpha}(x)$ une fonction entière.

Soient maintenant b une seconde racine de $f(x)=0$ et β son degré de multiplicité, en sorte que l'on ait

$$f_1(x)=(x-b)^{\beta}f_2(x);$$

en appliquant la formule précédente à la fraction $\frac{F_{\alpha}(x)}{f_1(x)}$, on aura une valeur de la forme

$$\frac{F_{\alpha}(x)}{f_1(x)}=\frac{F_{\alpha}(x)}{(x-b)^{\beta}f_2(x)}=\frac{B}{(x-b)^{\beta}}+\frac{B_1}{(x-b)^{\beta-1}}+\ldots$$
$$+\frac{B_{\beta-1}}{x-b}+\frac{F_{\beta}(x)}{f_2(x)},$$

et, par suite,

$$\frac{F(x)}{f(x)} = \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a}$$
$$+ \frac{B}{(x-b)^6} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b} + \frac{F_6(x)}{f_2(x)},$$

B, B_1, etc., étant des constantes déterminées dont la première n'est pas nulle, et $F_6(x)$ une fonction entière.

Il résulte de là, qu'en général, si l'on suppose

$$f(x) = (x-a)^\alpha (x-b)^6 \ldots (x-c)^\gamma,$$

la fraction rationnelle $\frac{F(x)}{f(x)}$ pourra être décomposée de la manière suivante :

$$\frac{F(x)}{f(x)} = \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a},$$
$$+ \frac{B}{(x-b)^6} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \frac{C}{(x-c)^\gamma} + \frac{C_1}{(x-c)^{\gamma-1}} + \ldots + \frac{C_{\gamma-1}}{x-c} + E(x),$$

A, $A_1, \ldots$, B, $B_1, \ldots$, C, $C_1, \ldots$, étant des constantes finies, et $E(x)$ une fonction entière.

Au lieu de s'occuper d'abord des fractions simples relatives à la racine a, on aurait pu commencer par celles qui se rapportent à une autre racine, b par exemple ; mais, comme nous allons le faire voir, on aurait toujours trouvé le même résultat.

Théorème II. — *Une fraction rationnelle n'est dé-*

composable que d'une seule manière en une partie entière et en fractions simples.

Supposons qu'on ait trouvé ces deux valeurs d'une même fraction rationnelle $\frac{F(x)}{f(x)}$,

$$\frac{A}{(x-a)^\alpha}+\ldots+\frac{B}{(x-b)^\beta}+\ldots+E(x)$$

et

$$\frac{A'}{(x-a)^{\alpha'}}+\ldots+\frac{B'}{(x-b)^{\beta'}}+\ldots+E'(x);$$

on aura

$$\frac{A}{(x-a)^\alpha}+\ldots+E(x)=\frac{A'}{(x-a)^{\alpha'}}+\ldots+E'(x).$$

Cela posé, α et α' étant respectivement les exposants des plus hautes puissances de $x-a$, dans les deux membres, je dis que $\alpha=\alpha'$ et $A=A'$. Supposons, en effet, que α et α' soient inégaux et que α soit le plus grand; tirons de l'équation précédente la valeur de $\frac{A}{(x-a)^\alpha}$, et réduisons tous les autres termes au même dénominateur; on aura

$$\frac{A}{(x-a)^\alpha}=\frac{\varphi(x)}{(x-a)^{\alpha-1}\psi(x)},$$

ou

$$A=(x-a)\frac{\varphi(x)}{\psi(x)},$$

φ et ψ désignant des polynômes dont le second n'est pas divisible par $x-a$. D'ailleurs, A est une constante; il faut donc qu'elle soit nulle, car l'équation précédente donne $A=0$ pour $x=a$. Si donc A n'est pas nul, on ne peut supposer $\alpha>\alpha'$, et l'on ferait voir de même que, si A' n'est pas nul, on ne peut supposer non plus $\alpha<\alpha'$; on a donc $\alpha=\alpha'$. Je dis maintenant que $A=A'$. En effet, de

l'équation entre les deux valeurs de $\frac{F(x)}{f(x)}$, on tirera, α' étant égal à α,

$$\frac{A - A'}{(x-a)^\alpha} = \frac{\varphi(x)}{(x-a)^{\alpha-1}\psi(x)},$$

ou

$$A - A' = (x-a)\frac{\varphi(x)}{\psi(x)},$$

φ et ψ étant, comme précédemment, des polynômes dont le second n'est pas divisible par $x - a$; comme $A - A'$ est constant, et que sa valeur est nulle pour $x = a$, d'après l'équation précédente, on aura $A = A'$.

Les termes qui renferment la plus haute puissance de $x - a$ en dénominateur, dans les deux valeurs de la fraction rationnelle, étant égaux entre eux, on pourra les ôter de part et d'autre, et les deux restes seront égaux. En raisonnant de même sur ces deux restes, on fera voir que les termes qui contiennent en dénominateur la plus haute puissance du même binôme $x - a$, ou d'un autre binôme, sont aussi égaux entre eux; et en continuant ainsi, on prouvera que les fractions simples des deux valeurs de $\frac{F(x)}{f(x)}$ sont égales chacune à chacune: il en résultera, par conséquent, l'égalité des parties entières $E(x)$ et $E'(x)$.

Corollaire. — La partie entière qui entre dans la valeur d'une fraction rationnelle $\frac{F(x)}{f(x)}$ décomposée en fractions simples étant indépendante du moyen qu'on emploie pour effectuer la décomposition, on obtiendra cette partie entière en faisant la division de $F(x)$ par $f(x)$; car si $\varphi(x)$ désigne le reste de cette division, $E(x)$ le quotient, on aura

$$\frac{F(x)}{f(x)} = E(x) + \frac{\varphi(x)}{f(x)}.$$

Or, le degré de $\varphi(x)$ étant moindre que celui de $f(x)$, la valeur de $\frac{\varphi(x)}{f(x)}$ ne contiendra évidemment pas de partie entière; donc, etc.

Méthodes pour effectuer la décomposition d'une fraction rationnelle en fractions simples.

Le corollaire du théorème I, par lequel on démontre la possibilité de la décomposition, donne aussi le moyen de l'effectuer. Ainsi, dans le cas où les exposants $\alpha, \beta, \ldots, \gamma$ se réduisent tous à l'unité, on en déduit aisément la formule que nous avons obtenue dans la leçon précédente; mais, ce cas simple excepté, l'emploi de ce procédé exigerait des calculs fort pénibles.

On peut aussi employer la méthode des coefficients indéterminés; il faut alors calculer la partie entière en divisant le numérateur de la fraction proposée par le dénominateur, ainsi que nous l'avons déjà dit plus haut; on n'aura plus ensuite qu'à décomposer une fraction, dont le numérateur est de degré inférieur à celui du dénominateur; on égalera cette fraction à la somme des fractions simples dans lesquelles elle est susceptible de se décomposer, et dont les numérateurs constants sont les seules inconnues; on chassera les dénominateurs, et en égalant les coefficients des mêmes puissances de x dans les deux membres, on obtiendra une série d'équations qui serviront à déterminer les inconnues.

Exemple. — Soit à décomposer la fraction rationnelle $\frac{1}{x^3(x-1)}$ en fractions simples.

On posera

$$\frac{1}{x^3(x-1)} = \frac{A}{x^3} + \frac{B}{x^2} + \frac{C}{x} + \frac{D}{x-1},$$

d'où, en chassant les dénominateurs,

$$\begin{aligned}1 &= A(x-1) + B(x^2-x) + C(x^3-x^2) + Dx^3\\ &= -A + (A-B)x + (B-C)x^2 + (C+D)x^3,\end{aligned}$$

et, par conséquent,

$$-A = 1, \quad A - B = 0, \quad B - C = 0, \quad C + D = 0,$$

d'où

$$A = -1, \quad B = -1, \quad C = -1, \quad D = 1,$$

et, par suite,

$$\frac{1}{x^3(x-1)} = -\frac{1}{x^3} - \frac{1}{x^2} - \frac{1}{x} + \frac{1}{x-1}.$$

Nous allons indiquer une autre méthode qui n'exige que l'emploi de la division algébrique.

Soit la fraction rationnelle $\frac{F(x)}{f(x)}$, dont le dénominateur $f(x)$ a pour valeur

$$f(x) = (x-a)^\alpha (x-b)^6 \ldots (x-c)^\gamma;$$

cette fraction n'étant susceptible que d'une seule décomposition, on peut chercher, à part la partie entière, les fractions simples qui répondent à la racine a, puis celles qui répondent à la racine b, etc., et faire ensuite la somme de tous les résultats partiels ainsi obtenus.

La partie entière $E(x)$ s'obtiendra par la division de $F(x)$ par $f(x)$; voyons comment on peut obtenir les fractions simples qui répondent à chaque racine, à a par exemple. Soit

$$f(x) = (x-a)^\alpha f_1(x).$$

Posons $x = a + h$, ordonnons les polynômes $F(a+h)$ et $f_1(a+h)$ par rapport aux puissances croissantes de h, et faisons la division du premier par le second, en arrêtant le quotient au terme du degré $\alpha - 1$ en h; soient

$$A + A_1 h + A_2 h^2 + \ldots + A_{\alpha-1} h^{\alpha-1}$$

ce quotient, et $h^\alpha R$ le reste qui contient h^α à tous ses termes, en sorte que R désigne ici une fonction entière de h; on aura

$$\frac{F(a+h)}{f_1(a+h)} = A + A_1 h + A_2 h^2 + \ldots + A_{\alpha-1} h^{\alpha-1} + \frac{h^\alpha R}{f_1(a+h)}.$$

Remplaçons dans cette égalité h par sa valeur $x-a$, puis divisons les deux membres par $(x-a)^\alpha$, et remarquons enfin que R se réduira à une fonction entière de x, $F_\alpha(x)$; on aura

$$\frac{F(x)}{f(x)} = \frac{F(x)}{(x-a)^\alpha f_1(x)}$$

$$= \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \frac{A_2}{(x-a)^{\alpha-2}} + \ldots + \frac{A_{\alpha-1}}{x-a} + \frac{F_\alpha(x)}{f_1(x)};$$

d'où il suit que la partie de la valeur de $\frac{F(x)}{f(x)}$, qui est relative à la racine a, sera

$$\frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a}.$$

On pourrait déterminer ainsi, indépendamment les unes des autres, les fractions qui se rapportent aux diverses racines, mais il sera plus simple d'appliquer la même méthode à la fraction $\frac{F_\alpha(x)}{f_1(x)}$ qui complète les termes déjà trouvés; on obtiendra ainsi les termes qui se rapportent à une seconde racine, et une troisième fraction sur laquelle on continuera l'opération.

La méthode précédente a surtout l'avantage de faire connaître l'expression algébrique des numérateurs des diverses fractions simples dans lesquelles se décompose la fraction rationnelle proposée. En effet, la division des polynômes $F(a+h)$ et $f_1(a+h)$, que nous avons effec-

tuée, dans le but d'obtenir les coefficients $A_1, A_2, \ldots, A_\alpha$, revient évidemment à développer la fonction $\frac{F(a+h)}{f_1(a+h)}$ en série ordonnée suivant les puissances croissantes de h, et comme une fonction n'est développable que d'une seule manière en une série de cette espèce, on obtiendra le même résultat en faisant usage de la formule de Maclaurin. Si donc on pose

$$\frac{F(x)}{f_1(x)} = \varphi(x),$$

on aura

$$\frac{F(a+h)}{f_1(a+h)} = \varphi(a+h) = \varphi(a) + h\varphi'(a) + h^2\frac{\varphi''(a)}{1.2} + \ldots$$
$$+ h^{\alpha-1}\frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)} + h^\alpha R_1,$$

en désignant par $h^\alpha R_1$ le reste de la série; ici R_1 est une fonction rationnelle de h qui n'est point infinie pour $h = 0$, et, par conséquent, cette valeur de $\frac{F(a+h)}{f_1(a+h)}$ est identique à celle trouvée précédemment. On aura donc

$$A = \varphi(a),\quad A_1 = \varphi'(a),\quad A_2 = \frac{\varphi''(a)}{1.2}, \ldots,$$
$$A_{\alpha-1} = \frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)},$$

d'où résulte ce théorème général.

Théorème. — *Si l'on a*

$$f(x) = (x-a)^\alpha(x-b)^6\ldots(x-c)^\gamma,$$

que $F(x)$ *désigne une fonction entière de* x, *dont le quotient par* $f(x)$ *soit* $E(x)$, *et que l'on fasse, pour*

abréger,

$$\varphi(x) = (x-a)^\alpha \frac{F(x)}{f(x)}, \quad \psi(x) = (x-b)^6 \frac{F(x)}{f(x)}, \ldots,$$
$$\varpi(x) = (x-c)^\gamma \frac{F(x)}{f(x)},$$

on aura la valeur suivante de la fraction rationnelle $\frac{F(x)}{f(x)}$:

$$\frac{F(x)}{f(x)} = E(x)$$

$$+\frac{\varphi(a)}{(x-a)^\alpha} + \frac{\varphi'(a)}{(x-a)^{\alpha-1}} + \frac{\varphi''(a)}{1.2(x-a)^{\alpha-2}} + \ldots + \frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)(x-a)}$$

$$+\frac{\psi(b)}{(x-b)^6} + \frac{\psi'(b)}{(x-b)^{6-1}} + \frac{\psi''(b)}{1.2(x-b)_{6-2}} + \ldots + \frac{\psi^{6-1}(b)}{1.2\ldots(6-1)(x-b)}$$

....

....

$$+\frac{\varpi(c)}{(x-c)^\gamma} + \frac{\varpi'(c)}{(x-c)^{\gamma-1}} + \frac{\varpi''(c)}{1.2(x-c)^{\gamma-2}} + \ldots + \frac{\varpi^{\gamma-1}(c)}{1.2\ldots(\gamma-1)(x-c)}.$$

Ce résultat est susceptible d'une autre forme très-simple et très-élégante, ainsi qu'on peut le voir dans la Note IV.

La théorie qui vient d'être exposée subsiste entièrement si quelques-unes des racines de $f(x) = 0$ sont imaginaires, mais la valeur de $\frac{F(x)}{f(x)}$ est alors compliquée d'imaginaires. On a cherché à modifier, dans ce cas, la manière d'effectuer la décomposition de façon à n'introduire que des quantités réelles, et on y est parvenu par une méthode que nous exposerons dans la leçon suivante.

SEPTIÈME LEÇON.

Mode particulier de décomposition des fractions rationnelles dont le dénominateur a des facteurs linéaires imaginaires. — Conditions pour que l'intégrale d'une différentielle rationnelle soit algébrique. — Détermination du terme général d'une série récurrente.

Mode particulier de décomposition des fractions rationnelles dont le dénominateur a des facteurs linéaires imaginaires.

La possibilité du nouveau mode de décomposition, que nous avons en vue, résulte du théorème suivant :

Théorème I. — *Si $x^2 + px + q$ est le produit de deux facteurs imaginaires conjugués du polynôme réel $f(x)$, n la plus haute puissance de ce trinôme qui divise $f(x)$, en sorte qu'on ait*

$$f(x) = (x^2 + px + q)^n f_1(x),$$

la fraction réelle et rationnelle $\frac{F(x)}{f(x)}$ pourra se décomposer en deux parties, de la manière suivante :

$$\frac{F(x)}{f(x)} = \frac{Px + Q}{(x^2 + px + q)^n} + \frac{F_1(x)}{(x^2 + px + q)^{n-1} f_1(x)},$$

P *et* Q *étant des constantes réelles, et* $F_1(x)$ *un polynôme réel.*

En effet, on a identiquement

$$\frac{F(x)}{f(x)} = \frac{F(x)}{(x^2 + px + q)^n f_1(x)}$$
$$= \frac{Px + Q}{(x^2 + px + q)^n} + \frac{F(x) - (Px + Q) f_1(x)}{(x^2 + px + q)^n f_1(x)};$$

et l'on peut déterminer P et Q de manière que le numérateur de la deuxième partie du second membre soit divisible par $x^2 + px + q$, c'est-à-dire de manière que ce numérateur s'annule en remplaçant x par chacune des racines de l'équation

$$x^2 + px + q = 0.$$

Soient $h + k\sqrt{-1}$ et $h - k\sqrt{-1}$ ces deux racines, et posons

$$F(h \pm k\sqrt{-1}) - [P(h \pm k\sqrt{-1}) + Q] f_1(h \pm k\sqrt{-1}) = 0;$$

on tirera de là

$$P(h \pm k\sqrt{-1}) + Q = \frac{F(h \pm k\sqrt{-1})}{f_1(h \pm k\sqrt{-1})} = M \pm N\sqrt{-1}),$$

M et N étant des quantités réelles dont les valeurs sont finies et déterminées, puisque, par hypothèse, $f_1(x)$ n'est pas divisible par $x^2 + px + q$. L'équation précédente se décompose dans les deux suivantes :

$$Ph + Q = M, \quad Pk = N,$$

qui donnent pour P et Q ces deux valeurs réelles et finies,

$$P = \frac{N}{k}, \quad Q = \frac{Mk - Nh}{k}.$$

Les valeurs de P et Q étant ainsi déterminées, nous poserons

$$\frac{F(x) - (Px + Q) f_1(x)}{x^2 + px + q} = F_1(x),$$

$F_1(x)$ désignant un polynôme réel, et, par suite, on aura

$$\frac{F(x)}{(x^2+px+q)^n f_1(x)} = \frac{Px + Q}{(x^2+px+q)^n} + \frac{F_1(x)}{(x^2+px+q)^{n-1} f_1(x)};$$

ce qu'il fallait démontrer.

Corollaire. — On voit par là que la fraction rationnelle $\frac{F(x)}{f(x)}$ pourra se décomposer de la manière suivante :

$$\frac{F(x)}{f(x)} = \frac{Px+Q}{(x^2+px+q)^n} + \frac{P_1x+Q_1}{(x^2+px+q)^{n-1}} + \ldots$$
$$+ \frac{P_{n-1}x+Q_{n-1}}{x^2+px+q} + \frac{F_n(x)}{f_1(x)},$$

P, Q, P_1, Q_1, etc., désignant des constantes réelles, et $F_n(x)$ un polynôme réel aussi. Et en combinant le théorème précédent avec le théorème analogue démontré dans la dernière leçon, on obtient celui-ci :

Théorème II. — *Si l'on décompose le polynôme $f(x)$ en facteurs réels du premier et du second degré, en sorte qu'on ait*

$$f(x) = (x-a)^\alpha (x-b)^6 \ldots (x-c) \; (x^2+px+q)^n \ldots (x^2+rx+s)^m,$$

on pourra décomposer la fraction rationnelle $\frac{F(x)}{f(x)}$ de la manière suivante :

$$\frac{F(x)}{f(x)} = E(x) + \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a};$$
$$+ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$+ \frac{C}{(x-c)^\gamma} + \frac{C_1}{(x-c)^{\gamma-1}} + \ldots + \frac{C_{\gamma-1}}{x-c}$$
$$+ \frac{Px+Q}{(x^2+px+q)^n} + \frac{P_1x+Q_1}{(x^2+px+q)^{n-1}} + \ldots + \frac{P_{n-1}x+Q_{n-1}}{x^2+px+q}$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$+ \frac{Rx+S}{(x^2+rx+s)^m} + \frac{R_1x+S_1}{(x^2+rx+s)^{m-1}} + \ldots + \frac{R_{m-1}x+S_{m-1}}{x^2+rx+s},$$

$E(x)$ désignant une partie entière qui peut être nulle, et A, A_1, ..., C, C_1, ..., P, Q, P_1, Q_1, ..., R, S, R_1, S_1, ..., *des constantes réelles.*

Théorème III. — *Une fraction rationnelle n'est décomposable que d'une seule manière en fractions simples de la forme qu'on vient de considérer.*

Soient deux valeurs d'une même fraction rationnelle $\frac{F(x)}{f(x)}$. On démontrera, comme nous l'avons fait dans la leçon précédente, l'égalité des fractions simples qui correspondent aux facteurs du premier degré du dénominateur, et quant à celles des fractions simples qui correspondent aux facteurs du second degré, elle peut se démontrer d'une manière analogue, comme nous allons voir. Soient $\frac{Px+Q}{(x^2+px+q)^n}$ le terme dont le dénominateur contient la plus haute puissance de x^2+px+q dans la première valeur de $\frac{F(x)}{f(x)}$, et $\frac{P'x+Q'}{(x^2+px+q)^{n'}}$ le terme analogue dans la seconde valeur. Je dis d'abord que $n'=n$. Supposons, en effet, que cela ne soit pas, et que $n>n'$: de l'égalité qui a lieu entre les deux valeurs de $\frac{F(x)}{f(x)}$, tirons la valeur de $\frac{Px+Q}{(x^2+px+q)^n}$; cette valeur sera exprimée par une somme de quantités dont aucune n'a en dénominateur une puissance de x^2+px+q supérieure à $n-1$. En réduisant donc toutes ces quantités au même dénominateur, on aura une égalité de la forme

$$\frac{Px+Q}{(x^2+px+q)^n}=\frac{\varphi(x)}{(x^2+px+q)^{n-1}\psi(x)},$$

ou

$$Px+Q=(x^2+px+q)\frac{\varphi(x)}{\psi(x)},$$

$\varphi(x)$ et $\psi(x)$ désignant des polynômes, dont le second $\psi(x)$ n'est pas divisible par x^2+px+q. Or l'égalité

précédente est impossible; car, autrement, l'équation $Px+Q=0$ devrait admettre les deux racines de l'équation $x^2+px+q=0$, ce qui ne peut arriver, à moins que P et Q ne soient nuls en même temps, contrairement à l'hypothèse. On ne peut donc supposer $n>n'$ ni $n'>n$, pour une raison semblable; par conséquent, on a $n'=n$.

Je dis maintenant que l'on a aussi $P'=P$, $Q'=Q$. Reprenons, en effet, l'égalité qui a lieu par hypothèse entre les deux valeurs de $\frac{F(x)}{f(x)}$, mettons dans un même membre les deux termes $\frac{Px+Q}{(x^2+px+q)^n}$ et $\frac{P'x+Q'}{(x^2+px+q)^n}$, et dans le second membre tous les autres termes dont les dénominateurs ne contiendront aucune puissance de x^2+px+q supérieure à la $(n-1)^{ième}$; réduisant tous ces derniers termes au même dénominateur, on aura une égalité de cette forme

$$\frac{(P-P')x+(Q-Q')}{(x^2+px+q)^n}=\frac{\varphi(x)}{(x^2+px+q)^{n-1}\psi(x)},$$

ou

$$(P-P')x+(Q-Q')=(x^2+px+q)\frac{\varphi(x)}{\psi(x)},$$

$\varphi(x)$ et $\psi(x)$ désignant, comme précédemment, des polynômes dont le second n'est pas divisible par x^2+px+q, et l'on fera voir aussi, comme plus haut, que cette égalité exige

$$P=P',\quad Q=Q'.$$

Il suit de là que dans les deux valeurs de $\frac{F(x)}{f(x)}$, les termes qui contiennent en dénominateur la plus haute puissance d'un facteur du second degré sont égaux; en supprimant

ces deux termes, les deux restes auront encore, pour la même raison, deux termes égaux; et, en continuant ainsi, on voit que les deux valeurs de la fraction considérée ne sont formées que de fractions simples égales chacune à chacune : il en résulte en même temps l'égalité des parties entières, s'il y en a.

Méthode de décomposition. — Pour effectuer la décomposition d'une fraction rationnelle $\frac{F(x)}{f(x)}$, on déterminera la partie entière et les fractions qui correspondent aux facteurs réels du premier degré du dénominateur, comme on l'a vu dans la leçon précédente. Quant aux fractions qui correspondent aux facteurs réels du second degré, on pourra les déterminer successivement par le procédé même qui nous a servi à démontrer le théorème I. On pourra aussi faire usage de la méthode des coefficients indéterminés.

Dans le cas où les racines imaginaires de l'équation $f(x)=0$ sont toutes inégales, on peut déduire la nouvelle expression de la fraction rationnelle $\frac{F(x)}{f(x)}$ de celle qui a été établie dans la cinquième leçon. Soient, en effet, $h+k\sqrt{-1}$ et $h-k\sqrt{-1}$ deux racines simples imaginaires et conjuguées de l'équation $f(x)=0$; l'expression de la fraction $\frac{F(x)}{f(x)}$ contiendra, comme on l'a vu dans la cinquième leçon, les deux termes suivants :

$$\frac{F(h+k\sqrt{-1})}{f'(h+k\sqrt{-1})}\frac{1}{x-h-k\sqrt{-1}},$$

$$\frac{F(h-k\sqrt{-1})}{f'(h-k\sqrt{-1})}\frac{1}{x-h+k\sqrt{-1}}.$$

La somme de ces deux termes est de la forme

$$\frac{P+Q\sqrt{-1}}{x-h-k\sqrt{-1}}+\frac{P-Q\sqrt{-1}}{x-h+k\sqrt{-1}},$$

ou, en réduisant les deux fractions au même dénominateur, de la forme

$$\frac{Px+Q}{(x-h)^2+k^2};$$

d'où il suit que la fraction $\frac{Px+Q}{(x-h)^2+k^2}$, où P et Q désignent des constantes réelles, pourra remplacer, dans l'expression de $\frac{F(x)}{f(x)}$, les deux fractions simples qui correspondent aux racines $h\pm k\sqrt{-1}$.

Conditions pour que l'intégrale d'une différentielle rationnelle soit algébrique.

L'une des applications les plus importantes de la théorie qui vient d'être exposée, est l'intégration des différentielles rationnelles. Nous n'avons point à nous occuper ici des détails de cette intégration, et nous nous bornerons à donner les conditions pour qu'une différentielle rationnelle ait une intégrale algébrique.

Soit une différentielle rationnelle

$$\frac{F(x)}{f(x)}dx,$$

et

$$f(x)=(x-a)^{\alpha}(x-b)^{6}\ldots(x-c)^{\gamma},$$

$a, b, \ldots, c$ étant des quantités réelles ou imaginaires; on

mettra la fraction $\frac{F(x)}{f(x)}$ sous la forme

$$\frac{F(x)}{f(x)} = E(x) + \frac{A}{(x-a)^\alpha} + \frac{A_1}{(x-a)^{\alpha-1}} + \ldots + \frac{A_{\alpha-1}}{x-a}$$
$$+ \frac{B}{(x-b)^6} + \frac{B_1}{(x-b)^{6-1}} + \ldots + \frac{B_{6-1}}{x-b}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \frac{C}{(x-c)^\gamma} + \frac{C}{(x-c)^{\gamma-1}} + \ldots + \frac{C_{\gamma-1}}{x-c}.$$

Pour avoir l'intégrale de $\frac{F(x)}{f(x)}dx$, il faut multiplier par dx chaque terme de cette valeur de $\frac{F(x)}{f(x)}$, et intégrer tous les résultats. Or, les seuls parmi ces résultats dont l'intégrale n'est pas algébrique sont ceux qui ont pour dénominateur la première puissance de l'un des binômes $x-a$, $x-b$, etc.

On a en effet, si α' n'est pas égal à 1,

$$\int \frac{A\,dx}{(x-a)^{\alpha'}} = -\frac{A}{\alpha'(x-a)^{\alpha'-1}} + \text{constante},$$

et, si $\alpha' = 1$,

$$\int \frac{A\,dx}{x-a} = A \log(x-a) + \text{constante}.$$

Donc, pour que $\frac{F(x)}{f(x)}dx$ ait une intégrale algébrique, il faut et il suffit que, dans le développement de $\frac{F(x)}{f(x)}$ en fractions simples, il n'y ait aucun terme dont le dénominateur

soit du premier degré, c'est-à-dire que l'on ait

$$A_{\alpha-1}=0,\quad B_{6-1}=0,\ldots,\quad C_{\gamma-1}=0.$$

Cela exige d'abord que le polynôme $f(x)$ ne contienne aucun facteur linéaire simple. Nous avons vu, dans la leçon précédente, qu'en posant

$$\varphi(x)=(x-a)^{\alpha}\frac{F(x)}{f(x)},\quad \psi(x)=(x-b)^{6}\frac{F(x)}{f(x)},\ldots,$$

$$\varpi(x)=(x-c)^{\gamma}\frac{F(x)}{f(x)},$$

on a

$$A_{\alpha-1}=\frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)},\quad B_{6-1}=\frac{\psi^{6-1}(b)}{1.2\ldots(6-1)},\ldots,$$

$$C_{\gamma-1}=\frac{\varpi^{\gamma-1}(c)}{1.2\ldots(\gamma-1)};$$

les conditions pour que $\int\frac{F(x)}{f(x)}dx$ soit algébrique, sont donc

$$\varphi^{\alpha-1}(a)=0,\quad \psi^{6-1}(b)=0,\ldots,\quad \varpi^{\gamma-1}(c)=0,$$

quelles que soient les quantités a, b,..., c, réelles ou imaginaires.

Ces conditions sont en même nombre que les racines a, b,..., c; mais si le degré de $F(x)$ est inférieur de deux unités au moins de celui de $f(x)$, l'une d'elles sera comprise dans les autres. Désignons, en effet, par m le degré de $f(x)$, et supposons que $F(x)$ soit au plus du degré $m-2$; la partie entière $E(x)$ de $\frac{F(x)}{f(x)}$ sera nulle, et si l'on réduit au même dénominateur toutes les fractions simples, pour les ajouter et recomposer la fraction

$\frac{F(x)}{f(x)}$, on voit, sans peine, que le numérateur de la fraction ainsi obtenue contiendra x^{m-1} avec le coefficient

$$A_{\alpha-1} + B_{6-1} + \ldots + C_{\gamma-1}.$$

Ce coefficient doit être nul, puisque $F(x)$ est du degré $m-2$ au plus ; on a donc

$$\frac{\varphi^{\alpha-1}(a)}{1.2\ldots(\alpha-1)} + \frac{\psi^{6-1}(b)}{1.2\ldots(6-1)} + \ldots + \frac{\varpi^{\gamma-1}(c)}{1.2\ldots(\gamma-1)} = 0;$$

et, par conséquent, l'une des conditions pour que $\int \frac{F(x)}{f(x)}dx$ soit algébrique rentrera dans les autres.

L'équation précédente comprend, comme cas particulier, une formule démontrée dans la cinquième leçon, et sur laquelle nous avons eu occasion de nous appuyer.

J'indiquerai une seconde application importante de la théorie des fractions rationnelles : elle est relative à la théorie des séries récurrentes.

Détermination du terme général d'une série récurrente.

Lorsqu'on divise l'un par l'autre deux polynômes $F(x)$ et $f(x)$ ordonnés par rapport aux puissances croissantes de x, et que l'opération ne se termine pas, le quotient forme une série dite *récurrente,* que l'on obtiendrait aussi en développant la fonction $\frac{F(x)}{f(x)}$ en série, par la formule de Maclaurin, ou par tout autre moyen ; car on sait qu'une fonction n'est développable que d'une seule manière en série ordonnée suivant les puissances de la variable. On trouvera dans la Note I une formule remarquable de Lagrange dont on peut se servir pour cet objet. Mais le pro-

cédé que nous allons indiquer ici est, dans bien des cas, celui qu'on devra préférer.

Décomposons la fraction $\frac{F(x)}{f(x)}$ en fractions simples, en adoptant le mode de décomposition indiqué dans la leçon précédente, et supposons que l'on trouve de cette manière

$$\frac{F(x)}{f(x)} = E(x) + \sum \frac{A}{(x-a)^\alpha}.$$

Pour résoudre la question que nous nous proposons, il suffit de développer en série, par la formule du binôme, chacune des fractions simples $\frac{A}{(x-a)^\alpha}$ ou $A(x-a)^{-\alpha}$.

On a ainsi

$$(x-a)^{-\alpha} = (-a)^{-\alpha}\left(1-\frac{x}{a}\right)^{-\alpha}$$

$$= (-a)^{-\alpha}\left[\begin{array}{l} 1 + \frac{\alpha}{1}\frac{x}{a} + \frac{\alpha(\alpha+1)}{1.2}\frac{x^2}{a^2} + \ldots \\ + \frac{\alpha(\alpha+1)\ldots(\alpha+n-1)}{1.2\ldots n}\frac{x^n}{a^n} + \ldots \end{array}\right];$$

et si ρ_n désigne le coefficient de x^n dans $E(x)$, le terme général du développement de $\frac{F(x)}{f(x)}$ en série sera

$$x^n\left[\rho_n + \sum (-1)^\alpha \frac{\alpha(\alpha+1)\ldots(\alpha+n-1)}{1.2.3\ldots n}\frac{A}{a^{\alpha+n}}\right].$$

Dans le cas particulier où les racines a, etc., de $f(x)=0$ sont toutes simples, on a $\alpha = 1$ et $A = \frac{F(a)}{f'(a)}$; le terme général se réduit à

$$x^n\left[\rho_n - \sum \frac{F(a)}{a^{n+1} f'(a)}\right].$$

Ainsi la série récurrente dans laquelle se développe la fraction $\frac{F(x)}{f(x)}$ peut s'obtenir par l'addition de plusieurs séries provenant des développements de diverses puissances négatives et entières des binômes $a-x$, $b-x$, etc. D'ailleurs ces séries sont convergentes pour toutes les valeurs de x dont le module est inférieur au plus petit des modules des quantités a, b, etc.; d'où résulte ce théorème :

Théorème. — *Une série provenant du développement d'une fonction rationnelle* $\frac{F(x)}{f(x)}$ *est convergente pour toutes les valeurs réelles ou imaginaires de* x *dont le module est inférieur au plus petit module des racines de l'équation* $f(x)=0$.

Ce théorème a été généralisé par M. Cauchy et étendu à toutes les fonctions; on trouvera tous les développements que comporte cette importante question dans les *Exercices de Mathématiques* de M. Cauchy et dans le *Journal de Mathématiques* de M. Liouville.

Nous terminerons cette leçon par une application de la méthode qui vient d'être indiquée.

Exemple. — Proposons-nous de former la série récurrente dans laquelle se développe la fonction

$$\varphi(x)=\frac{P+Qx}{1-2x\cos\omega+x^2},$$

où P, Q et ω désignent des constantes données.

Décomposant cette fraction en fractions simples et employant, pour abréger l'écriture, la notation usuelle des exponentielles imaginaires, savoir,

$$e^{\pm\omega\sqrt{-1}}=\cos\omega\pm\sqrt{-1}\sin\omega,$$

on a

$$\varphi(x)=\frac{A}{1-xe^{\omega\sqrt{-1}}}+\frac{B}{1-xe^{-\omega\sqrt{-1}}},$$

A et B étant des constantes qui ont respectivement pour valeurs

$$A = \frac{Pe^{\omega\sqrt{-1}} + Q}{2\sin\omega\sqrt{-1}}, \quad B = \frac{Pe^{-\omega\sqrt{-1}} + Q}{2\sin\omega\sqrt{-1}}.$$

Développant en série chacune des parties de $\varphi(x)$, on trouve

$$\varphi(x) = A\sum x^n e^{n\omega\sqrt{-1}} - B\sum x^n e^{-n\omega\sqrt{-1}},$$

ou, en remplaçant A et B par leurs valeurs,

$$\varphi(x) = \sum \frac{(Pe^{\omega\sqrt{-1}} + Q)\,e^{n\omega\sqrt{-1}} - (Pe^{-\omega\sqrt{-1}} + Q)\,e^{-n\omega\sqrt{-1}}}{2\sin\omega\sqrt{-1}}\, x^n.$$

En remettant à la place des exponentielles imaginaires leurs valeurs, on a, toutes réductions faites,

$$\frac{P + Qx}{1 - 2x\cos\omega + x^2} = \sum \frac{P\sin(n+1)\omega + Q\sin n\omega}{\sin\omega}\, x^n.$$

Le terme général du développement est donc

$$\left(P\,\frac{\sin(n+1)\omega}{\sin\omega} + Q\,\frac{\sin n\omega}{\sin\omega}\right) x^n.$$

HUITIÈME LEÇON.

Des fonctions symétriques et rationnelles des solutions communes à plusieurs équations. — Extension de la méthode d'élimination par les fonctions symétriques, au cas d'un nombre quelconque d'équations. — Théorème de Bezout sur le degré de l'équation finale. — Méthode de Tschirnaüs, pour faire disparaître autant de termes que l'on veut d'une équation. — Application aux équations du troisième et du quatrième degré.

Nous avons exposé dans la troisième leçon une méthode fondée sur la théorie des fonctions symétriques, pour l'élimination d'une inconnue entre deux équations, et nous en avons déduit que le degré de l'équation finale est, au plus, égal au produit des degrés des deux équations données. Bezout a généralisé cette proposition en démontrant que *le degré de l'équation finale résultant de l'élimination de $k-1$ inconnues entre k équations est, au plus, égal au produit des degrés de ces équations.* Pour établir ce théorème, nous suivrons la marche indiquée par Poisson dans le onzième cahier du *Journal de l'École Polytechnique.* Nous commencerons par étendre au cas d'un nombre quelconque d'équations la méthode d'élimination par les fonctions symétriques, précédemment exposée pour le cas de deux équations seulement. Cette extension repose sur la considération des fonctions symétriques des solutions communes à plusieurs équations, fonctions dont nous allons d'abord nous occuper.

Pour éviter les difficultés que peuvent présenter quelques cas particuliers, je préviens, une fois pour toutes, que nous raisonnerons toujours, dans cette leçon, sur des

équations générales dont les coefficients demeurent indéterminés.

Toutes les conséquences auxquelles nous serons conduit auront lieu, en général, si l'on attribue aux coefficients des valeurs déterminées; mais nos raisonnements pourront être en défaut dans quelques cas particuliers.

Des fonctions symétriques et rationnelles des solutions communes à plusieurs équations.

Cas de deux équations. — Soient deux équations

$$f(x, y) = 0, \quad F(x, y) = 0,$$

entre les deux inconnues x et y, et

$$(x_1 y_1), \quad (x_2 y_2), \ldots, \quad (x_n y_n)$$

les couples de solutions communes à ces deux équations. On nomme *fonctions symétriques de ces solutions communes* toute fonction qui ne change pas de valeur, quand on y permute les groupes $(x_1 y_1)$, $(x_2 y_2)$, etc., les uns dans les autres; nous considérerons seulement les fonctions symétriques rationnelles. Une fonction de cette espèce est toujours exprimable rationnellement par les coefficients des équations proposées.

Par un raisonnement tout semblable à celui que nous avons fait au sujet des fonctions symétriques des racines d'une équation à une inconnue, on fera voir que la détermination d'une fonction rationnelle et symétrique des solutions $(x_1 y_1)$, $(x_2 y_2)$, etc., se ramène à celle de fonctions symétriques entières, homogènes, et dont les différents termes se déduisent les uns des autres, en changeant les indices des lettres x et y, mais sans changer leurs exposants. Les fonctions symétriques auxquelles on est ainsi ramené seront dites *simples* ou du premier ordre,

doubles ou du deuxième ordre, etc., suivant que chacun de leurs termes contiendra les lettres d'un, de deux, etc., groupes $(x_1 y_1)$, $(x_2 y_2)$, etc. La forme générale des fonctions simples sera

$$x_1^p y_1^q + x_2^p y_2^q + \ldots + x_n^p y_n^q,$$

p ou q pouvant être nul. Nous représenterons une pareille fonction par $\sum x_1^p y_1^q$. La forme des fonctions doubles sera

$$x_1^p y_1^q x_2^{p'} y_2^{q'} + x_1^p y_1^q x_3^{p'} y_3^{q'} + \ldots .$$

Nous la représenterons par $\sum x_1^p y_1^q x_2^{p'} y_2^{q'}$, et ainsi de suite.

Voici la méthode imaginée par Poisson pour calculer la fonction simple $\sum x_1^p y_1^q$.

Désignons par t une nouvelle variable, par α une indéterminée, et posons

$$t = x + \alpha y, \quad \text{d'où} \quad x = t - \alpha y;$$

en substituant cette valeur de x dans les équations proposées, celles-ci deviennent

$$f(t - \alpha y, y) = 0, \quad F(t - \alpha y, y) = 0,$$

et, en éliminant y, on a une équation finale en t,

$$\psi(t, \alpha) = 0,$$

qui contient dans ses différents termes l'indéterminée α. Cette équation en t a pour racines

$$x_1 + \alpha y_1, \quad x_2 + \alpha y_2, \ldots, \quad x_n + \alpha y_n,$$

et elle est, par conséquent, du degré n. D'ailleurs, la somme des puissances semblables de degré μ des racines de

l'équation en t peut s'exprimer rationnellement (première leçon) par les coefficients de cette équation, c'est-à-dire en fonction de α et des coefficients des équations proposées. On aura donc

$$(x_1 + \alpha y_1)^\mu + (x_2 + \alpha y_2)^\mu + \ldots + (x_n + \alpha y_n)^\mu$$
$$= A_0 + A_1 \alpha + A_2 \alpha^2 + \ldots,$$

où A_0, A_1, etc., désignent des quantités connues et exprimées rationnellement par les coefficients des équations proposées. Cette équation ayant lieu quel que soit α, les coefficients des mêmes puissances de α doivent être égaux dans les deux membres; d'où résulte cette suite d'égalités :

$$x_1^\mu + x_2^\mu + \ldots + x_n^\mu = A_0,$$

$$\frac{\mu}{1}\left(x_1^{\mu-1} y_1 + x_2^{\mu-1} y_2 + \ldots + x_n^{\mu-1} y_n\right) = A_1,$$

$$\frac{\mu(\mu-1)}{1.2}\left(x_1^{\mu-2} y_1^2 + x_2^{\mu-2} y_2^2 + \ldots + x_n^{\mu-2} y_n^2\right) = A_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1^\mu + y_2^\mu + \ldots + y_n^\mu = A_\mu,$$

qui feront connaître les fonctions simples $\sum x_1^p y_1^q$ de degré $p + q = \mu$.

Le calcul des fonctions doubles, triples, etc., se fait de la même manière que pour les fonctions symétriques ordinaires. Par exemple, pour avoir la fonction double $\sum x_1^p y_1^q x_2^{p'} y_2^{q'}$, on multipliera ensemble les deux fonctions simples $\sum x_1^p y_1^q$ et $\sum x_1^{p'} y_1^{q'}$; le produit se composera de la fonction simple $\sum x_1^{p+p'} y_1^{q+q'}$ et de la fonction

double qu'on veut trouver. On aura donc

$$\sum x_1^p y_1^q x_2^{p'} y_2^{q'} = \sum x_1^p y_1^q \sum x_1^{p'} y_1^{q'} - \sum x_1^{p+p'} y_1^{q+q'}.$$

Seulement, il faudrait ne prendre que la moitié de cette valeur, si l'on avait à la fois $p' = p$, $q' = q$.

Les fonctions triples, etc., se calculeront d'une manière analogue.

Ce qui précède suffit pour établir, comme nous l'avions annoncé, que les fonctions symétriques et rationnelles des solutions communes à deux équations peuvent s'exprimer rationnellement par les coefficients de ces équations, et l'on voit que leur détermination exige seulement l'élimination d'une inconnue entre deux équations.

Cas d'un nombre quelconque d'équations. — La même méthode s'applique à un nombre quelconque d'équations. Supposons, par exemple, qu'il s'agisse de trois équations à trois inconnues

$$f(x, y, z) = 0, \quad F(x, y, z) = 0, \quad \varphi(x, y, z) = 0,$$

et soient

$$(x_1, y_1, z_1), \quad (x_2, y_2, z_2), \ldots, \quad (x_n, y_n, z_n)$$

les groupes de solutions communes à ces trois équations. Conservant la classification que nous avons adoptée des diverses fonctions symétriques, la forme générale des fonctions simples sera

$$x_1^p y_1^q z_1^r + x_2^p y_2^q z_2^r + \ldots + x_n^p y_n^q z_n^r;$$

celle des fonctions doubles sera

$$x_1^p y_1^q z_1^r x_2^{p'} y_2^{q'} z_2^{r'} + \ldots,$$

et ainsi de suite. Et c'est à la détermination des pre-

mières que se ramène celle de toute fonction symétrique et rationnelle.

Désignant par t une nouvelle variable, par α et β deux indéterminées, nous poserons

$$t = x + \alpha y + \beta z, \quad \text{d'où} \quad x = t - \alpha y - \beta z.$$

Ayant substitué cette valeur de x dans les équations proposées, nous éliminerons y et z; nous obtiendrons ainsi une équation finale en t,

$$\psi(t, \alpha, \beta) = 0,$$

contenant les indéterminées α et β, et dont les racines seront

$$x_1 + \alpha y_1 + \beta z_1, \quad x_2 + \alpha y_2 + \beta z_2, \ldots, \quad x_n + \alpha y_n + \beta z_n.$$

La somme des puissances μ de ces racines pourra s'exprimer rationnellement par les coefficients de l'équation en t, c'est-à-dire en fonction des indéterminées α et β, et des coefficients des équations proposées. On aura ainsi une équation de la forme

$$\sum (x_1 + \alpha y_1 + \beta z_1)^\mu = \sum A_{q,r}\, \alpha^q \beta^r,$$

où le coefficient $A_{q,r}$ désigne généralement une quantité connue. Le signe sommatoire Σ du premier membre s'étend aux n racines de l'équation en t, celui du second membre à toutes les valeurs de q et de r, telles que

$$q + r = \quad \text{ou} \quad < \mu.$$

En posant $p = \mu - q - r$, et égalant les coefficients de $\alpha^q \beta^r$ dans les deux membres, on aura

$$\frac{1.2.3\ldots\mu}{(1.2\ldots p)(1.2\ldots q)(1.2\ldots r)} \sum x_1^p y_1^q z_1^r = A_{q,r};$$

c'est la formule qui fera connaître les fonctions simples.

Pour former les fonctions doubles, triples, etc., on procédera comme dans le cas de deux équations. La forme du calcul est la même, et l'on voit qu'en général les fonctions symétriques et rationnelles des solutions communes à plusieurs équations s'exprimeront toujours rationnellement par les coefficients de ces équations.

Il faut remarquer que la détermination des fonctions symétriques des solutions communes à trois équations exige l'élimination de deux inconnues entre trois équations, et généralement la détermination des fonctions symétriques des solutions communes à k équations exige l'élimination de $k-1$ inconnues entre k équations.

Extension de la méthode d'élimination par les fonctions symétriques, au cas d'un nombre quelconque d'équations.

La méthode que nous allons exposer, d'après Poisson, donne le moyen d'éliminer $k-1$ inconnues entre k équations, lorsqu'on sait éliminer $k-2$ inconnues entre $k-1$ équations, et, par conséquent, cette méthode ramène tous les cas, en dernière analyse, à l'élimination d'une inconnue entre deux équations.

Pour fixer les idées, nous considérerons quatre équations seulement, entre quatre ou un plus grand nombre d'inconnues; mais on verra sans peine que notre raisonnement est général et qu'il s'appliquerait sans modification au cas d'un nombre quelconque d'équations.

Soient donc les quatre équations

$$(1)\qquad \left\{\begin{array}{l} f(x,\ y,\ z,\ u,\ldots)=0,\\ F(x,\ y,\ z,\ u,\ldots)=0,\\ \varphi(x,\ y,\ z,\ u,\ldots)=0,\\ \Phi(x,\ y,\ z,\ u,\ldots)=0,\end{array}\right.$$

entre quatre ou un plus grand nombre d'inconnues x, y,

z, u, etc., et proposons-nous d'éliminer trois inconnues, x, y, z par exemple, entre ces quatre équations.

Considérons en particulier les trois premières des équations (1),

$$(2) \quad \begin{cases} f(x, y, z, u, \ldots) = 0, \\ F(x, y, z, u, \ldots) = 0, \\ \varphi(x, y, z, u, \ldots) = 0, \end{cases}$$

et, regardant x, y, z comme fonctions des autres variables u, etc., désignons par

$$(x_1, y_1, z_1), \quad (x_2, y_2, z_2), \ldots, \quad (x_n, y_n, z_n)$$

les n systèmes de solutions communes aux équations (2).

Cela posé, remplaçons (x, y, z), dans la quatrième des équations (1), successivement par chacun de ces n systèmes, et désignons par V le produit des résultats ainsi obtenus, en sorte qu'on ait

$$(3) \quad V = \Phi(x_1, y_1, z_1, u, \ldots)\,\Phi(x_2, y_2, z_2, u, \ldots)\ldots\Phi(x_n, y_n, z_n, u, \ldots);$$

l'équation

$$(4) \qquad V = 0$$

sera l'équation finale résultant de l'élimination de x, y et z entre les équations (1), car cette équation (4) exprime la condition nécessaire et suffisante pour que les équations (1) admettent un système (x, y, z) de solutions communes. D'ailleurs V est une fonction symétrique et entière des solutions communes aux équations (2); on pourra donc l'exprimer rationnellement par les quantités indépendantes de x, y, z qui entrent dans les équations (1). Pour cela, désignant, comme précédemment, par t une nouvelle variable, par α et 6 deux paramètres indéterminés, nous poserons

$$t = x + \alpha y + 6z, \quad \text{d'où} \quad x = t - \alpha y - 6z;$$

en substituant cette valeur de x dans les équations (2), on

aura les trois suivantes :

$$(5) \quad \begin{cases} f(t - \alpha y - 6z,\ y,\ z,\ u,\ldots) = 0, \\ F(t - \alpha y - 6z,\ y,\ z,\ u,\ldots) = 0, \\ \varphi(t - \alpha y - 6z,\ y,\ z,\ u,\ldots) = 0, \end{cases}$$

entre lesquelles il faudra éliminer y et z. C'est donc à l'élimination de deux inconnues entre trois équations que nous ramenons l'élimination de trois inconnues entre quatre équations. L'équation finale en t qui résulte de l'élimination de y et z entre les équations (5) aura pour racines

$$x_1 + \alpha y_1 + 6z_1,\quad x_2 + \alpha y_2 + 6z_2,\ldots,\quad x_n + \alpha y_n + 6z_n,$$

et sera, par conséquent, du degré n. Supposons-la formée, et ordonnons-la par rapport à t; elle sera

$$(6) \quad t^n + p_1 t^{n-1} + p_2 t^{n-2} + \ldots + p_{n-1} t + p_n = 0,$$

p_1, p_2, etc., étant des fonctions rationnelles de u, etc., qui contiennent aussi les paramètres α et 6. Cette équation (6) servira, comme nous l'avons vu précédemment, à calculer les diverses fonctions symétriques des solutions communes aux équations (2), dont l'expression de V est composée, et le problème sera enfin résolu.

Cette méthode conduirait, dans les applications, à des calculs d'une longueur rebutante; mais nous allons en conclure aisément la démonstration du théorème de Bezout, relatif au degré de l'équation finale, ce qui est l'objet principal que nous ayons en vue.

Théorème de Bezout sur le degré de l'équation finale.

D'après ce qui précède, n étant le nombre des solutions communes (x, y, z) aux équations (2), on obtiendra une équation finale du même degré n en éliminant deux inconnues quelconques entre les équations (2). Cela est

d'ailleurs évident à priori ; car, à cause de la généralité que nous supposons aux équations, tout est semblable par rapport à x, y, z, u, etc. Toutefois, il est important de faire cette remarque, parce que le contraire pourrait avoir lieu si l'on attribuait aux coefficients des valeurs particulières.

Lemme. — *Si n désigne le degré de l'équation finale qui résulte de l'élimination de deux inconnues entre les trois premières des équations* (1), *et m le degré de la quatrième équation* (1), *le degré de l'équation finale résultant de l'élimination de trois inconnues entre les quatre équations* (1) *est au plus égal à mn.*

L'équation (6), qui résulte de l'élimination de y et z entre les équations (5), étant du degré n, les coefficients p_1, p_2, etc., sont des fonctions entières de u, etc., dont la première est au plus du premier degré, la deuxième du second degré, etc. Cela posé, la somme des puissances semblables de degré μ des racines de l'équation (6), c'est-à-dire $\sum (x_1 + \alpha y_1 + 6 z_1)^\mu$, peut s'exprimer sous forme entière, en fonction des coefficients p_1, p_2, etc., par une formule qui est au plus du degré μ par rapport à u, etc. (*voir* première leçon) ; donc, une fonction symétrique simple, telle que $\sum x_1^p y_1^q z_1^r$, de degré $p + q + r = \mu$, s'exprimera par une formule qui sera elle-même au plus de ce degré μ, par rapport à u, etc. Il résulte de là, et du mode général suivant lequel les fonctions symétriques et entières les plus compliquées se forment à l'aide des fonctions simples, que toute fonction symétrique et entière de degré μ des solutions communes (x_1, y_1, z_1), etc., aux équations (2), s'exprimera par une formule entière qui sera au plus du degré μ par rapport à u, etc. Or chacun des termes de l'expression de V, donnée par l'équa-

tion (3), est le produit de puissances de u, etc., dont les exposants ont une somme $mn - \mu$ inférieure à mn, par une fonction symétrique entière de degré μ des solutions communes (x_1, y_1, z_1), etc., aux équations (2). Donc enfin, chacune de ces parties de V s'exprimera par une formule qui sera au plus du degré mn par rapport à u, etc., et, par suite, l'équation $V=0$ sera au plus du degré mn.

Remarque. — On pourrait faire à la démonstration précédente l'objection que voici : Le raisonnement suppose que les coefficients p_1, p_2, etc., sont entiers par rapport aux variables u, etc., ou, en d'autres termes, que l'équation (6), qui est du degré n par rapport à chacune des variables t, u, etc., soit de ce même degré par rapport à toutes les variables. Or cela n'est pas tout à fait évident, quoique les équations (1) ou (5) soient supposées chacune la plus générale de son degré. Voici, ce me semble, la manière la plus simple de lever cette objection. Si quelques-uns des coefficients p_1, p_2, etc., étaient fractionnaires, quelques-unes des racines t de l'équation (6) deviendraient infinies pour certaines valeurs finies des variables u, etc. Or je dis que cela ne peut avoir lieu, tant qu'on laisse indéterminés les coefficients des équations (2) ou (5), et il suffit évidemment, pour justifier cette assertion, de citer un cas où cela ne soit pas. Supposons qu'on donne aux coefficients des éqnations (5) des valeurs telles, que chacune, restant du même degré, se décompose en facteurs linéaires de la forme $t + ay + bz + cu + \ldots + l$: on pourra exprimer chacune des racines t de l'équation finale relative à ces équations particulières, en fonction de u, etc., par les formules qui servent à la résolution des équations du premier degré; et ces valeurs de t, étant évidemment de la forme $gu + \ldots + f$, ne pourront devenir infinies pour des valeurs finies de u, etc.

On déduit aisément du lemme qui précède la démonstration du théorème de Bezout.

THÉORÈME. — *Le degré de l'équation finale qui résulte de l'élimination de $k-1$ inconnues entre k équations est égal au produit des degrés de ces équations.*

Soient, en effet,

$$m_1, \ m_2, \ m_3, \ldots, \ m_k$$

les degrés de k équations. Le degré de l'équation finale résultant de l'élimination d'une inconnue entre les deux premières sera égal à m_1, m_2, ainsi que nous l'avons établi dans la troisième leçon : donc, d'après le lemme qui précède, si l'on élimine deux inconnues entre les trois premières équations, le degré de l'équation finale sera au plus $m_1 m_2 \times m_3$, ou $m_1 m_2 m_3$; de même, si l'on élimine trois inconnues entre les quatre premières, le degré de l'équation finale sera au plus $m_1 m_2 m_3 \times m_4$ ou $m_1 m_2 m_3 m_4$. Et l'on voit, en continuant ainsi, que le degré de l'équation finale qui résulte de l'élimination de $k-1$ inconnues entre les k équations sera au plus égal au produit des degrés de ces équations.

On peut même ajouter que le degré de l'équation finale sera précisément égal à ce produit, si les équations proposées sont chacune la plus générale de son degré, comme nous l'avons supposé. On s'en assure aisément en considérant un système de k équations décomposables chacune en facteurs linéaires, ainsi que nous l'avons fait dans la troisième leçon, pour le cas de deux équations.

COROLLAIRE. — Il résulte du théorème précédent et des développements exposés dans la quatrième leçon, que la résolution de plusieurs équations simultanées peut se ramener à la résolution d'une seule équation dont le degré est généralement égal au produit des degrés des proposées.

Méthode de Tschirnaüs, pour faire disparaître autant de termes que l'on veut d'une équation.

On peut rattacher à la théorie de l'élimination la méthode élégante que Tschirnaüs a donnée dans les *Actes de Leipsick* pour 1683, et qui sert à faire disparaître d'une équation autant de termes que l'on veut. Cette méthode consiste à transformer l'équation proposée en une autre dont la racine soit une fonction rationnelle de celle de la proposée, ou, si l'on veut, une fonction entière de degré inférieur à celui de l'équation proposée, car c'est à cette forme que peut se ramener la fonction rationnelle la plus générale (troisième leçon).

Soit

$$(1)\quad x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0$$

une équation du degré m, et posons

$$(2)\quad y = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} + a_n x^n,$$

a_0, a_1, etc., désignant des indéterminées, et n un entier inférieur à m. L'équation finale en y, qui résulte de l'élimination de x entre les équations (1) et (2), sera évidemment du degré m, puisque y a autant de valeurs que x. Cette élimination peut se faire par les fonctions symétriques, de la manière suivante : En élevant l'équation (2) aux différentes puissances 2, 3,..., m, et ayant soin de rabaisser les exposants de x au-dessous de m, à l'aide de l'équation (1), on aura une suite d'équations de la forme

$$(3)\quad \begin{cases} y^2 = b_0 + b_1 x + b_2 x^2 + \ldots + b_{m-1} x^{m-1}, \\ y^3 = c_0 + c_1 x + \ldots\ldots\ldots + c_{m-1} x^{m-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y^m = k_0 + k_1 x + \ldots\ldots \ldots + k_{m-1} x^{m-1}. \end{cases}$$

b_0, b_1, etc., sont des fonctions homogènes et entières du second degré des indéterminées a_0, a_1, etc.; pareillement c_0, c_1, etc., sont des fonctions homogènes et entières du troisième degré de a_0, a_1, etc., et ainsi de suite. Si, maintenant, s_1, s_2, etc., désignent les sommes de puissances semblables des racines de l'équation (1), S_1, S_2, etc., celles des puissances semblables des racines de l'équation en y, les équations (2) et (3) donneront

$$(4)\quad \left\{\begin{array}{l} S_1 = ma_0 + a_1 s_1 + a_2 s_2 + \ldots + a_{n-1} s_{n-1} + a_n s_n, \\ S_2 = mb_0 + b_1 s_1 + b_2 s_2 + \ldots\ldots\ldots + b_{m-1} s_{m-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S_m = mk_0 + k_1 s_1 + k_2 s_2 + \ldots\ldots\ldots + k_{m-1} s_{m-1}. \end{array}\right.$$

Connaissant ainsi les sommes de puissances semblables des racines de l'équation en y, on formera aisément cette équation.

On peut y arriver encore de la manière suivante. On résoudra les équations (3) par rapport aux puissances $x^1, x^2, \ldots, x^{m-1}$, et l'on portera leurs valeurs dans l'équation (2). Ce procédé a l'avantage de donner la valeur de x exprimée rationnellement en y, en sorte qu'on connaîtra chaque racine de l'équation proposée, quand on aura résolu l'équation finale en y.

Représentons par

$$(5)\quad y^m + q_1 y^{m-1} + q_2 y^{m-2} + \ldots + q_{m-1} y + q_m = 0$$

cette équation en y, où $q_1, q_2, \ldots, q_m$ sont fonctions des indéterminées a_0, a_1, etc., et qui exprime la condition pour que les équations (1) et (2) aient une racine commune. Je dis que de cette seule équation (5) on peut déduire la valeur de x qui correspond à chaque valeur de y, et même la valeur d'une puissance quelconque de x. En effet, y est une fonction des indéterminées a_0, a_1, etc.,

considérées comme des variables indépendantes, et l'on a alors

$$\frac{dy}{da_1} = x, \quad \frac{dy}{da_2} = x^2, \ldots .$$

Différentions maintenant l'équation (5) par rapport à a_1, dont y, q_1, q_2, etc., sont fonctions; on aura

$$[my^{m-1} + (m-1)\,q_1 y^{m-2} + \ldots + q_{m-1}]\,\frac{dy}{da_1}$$
$$+ \left(y^{m-1}\frac{dq_1}{da_1} + y^{m-2}\frac{dq_2}{da_1} + \ldots + \frac{dq_m}{da_1}\right) = 0,$$

et, par suite,

$$x = -\frac{y^{m-1}\dfrac{dq_1}{da_1} + y^{m-2}\dfrac{dq_2}{da_1} + \ldots + \dfrac{dq_m}{da_1}}{my^{m-1} + (m-1)\,q_1 y^{m-2} + \ldots + q_{m-1}}.$$

On trouverait de même, en différentiant, l'équation (5) par rapport à a_2,

$$x^2 = -\frac{y^{m-1}\dfrac{dq_1}{da_2} + y^{m-2}\dfrac{dq_2}{da_2} + \ldots + \dfrac{dq_m}{da_2}}{my^{m-1} + (m-1)\,q_1 y^{m-2} + \ldots + q^{m-1}},$$

et ainsi de suite.

On voit, par ce qui précède, qu'il suffira de résoudre l'équation (5) pour avoir résolu par cela même l'équation (1).

Cela posé, on peut disposer des indéterminées a_0, a_1, etc., de manière à faire évanouir n termes de l'équation en y, à partir du second par exemple. Il faudra alors, d'après les formules de Newton, que l'on ait

$$S_1 = 0, \quad S_2 = 0, \ldots, \quad S_n = 0.$$

Or, en se reportant aux équations (4), on voit que S_1 est du premier degré par rapport à a_0, a_1, etc., que S_2 est du deuxième, S_3 du troisième, etc., S_n du $n^{ième}$. Donc,

d'après le théorème de Bezout, la détermination de ces indéterminées, dont l'une peut être prise arbitrairement, dépend d'une équation du degré

$$1.2.3\ldots n;$$

et, si l'on voulait faire disparaître de l'équation (5) tous les termes, à l'exception du premier et du dernier, le problème dépendrait d'une équation du degré

$$1.2.3\ldots(m-1).$$

C'est aussi à la résolution d'une équation de ce degré que se trouverait ramenée celle de l'équation proposée, car l'équation (5) n'ayant alors que deux termes pourrait être immédiatement résolue.

Application aux équations du troisième et du quatrième degré.

Nous reviendrons, dans une prochaine leçon, sur la résolution des équations générales du troisième et du quatrième degré; mais nous ferons voir ici comment résulte immédiatement de la transformation de Tschirnaüs la possibilité d'effectuer cette résolution.

Soit d'abord l'équation du troisième degré

$$x^3 + px^2 + qx + r = 0;$$

on posera

$$y = a + bx + x^2,$$

et l'on formera l'équation finale en y, savoir

$$y^3 + Py^2 + Qy + R = 0.$$

On déterminera a et b à l'aide des équations $P = 0$, $Q = 0$, qui sont, l'une du premier degré, l'autre du second; on pourra donc les résoudre et exprimer a et b en fonction des coefficients de la proposée. L'équation en y

se réduisant alors à

$$y^3 + R = 0,$$

on en tirera ces trois valeurs

$$y = \sqrt[3]{-R}, \quad y = \alpha\sqrt[3]{-R}, \quad y = 6\sqrt[3]{-R},$$

α et 6 désignant les racines cubiques imaginaires de 1. Connaissant ainsi les trois valeurs de y, on aura facilement, par ce que nous avons dit plus haut, les trois valeurs de x.

Soit enfin l'équation du quatrième degré

$$x^4 + px^3 + qx^2 + rx + s = 0;$$

on posera, comme précédemment,

$$y = a + bx + x^2,$$

et l'on aura une équation en y telle, que

$$y^4 + Py^3 + Qy^2 + Ry + S = 0.$$

On déterminera a et b à l'aide des équations $P = 0$, $R = 0$, qui sont, l'une du premier degré, l'autre du troisième; on pourra donc résoudre ces équations et exprimer a et b en fonction des coefficients de la proposée. L'équation en y, se réduisant à

$$y^4 + Qy^2 + S = 0,$$

pourra elle-même être résolue, puisqu'elle est bicarrée. Connaissant les quatre valeurs de y, on aura aussi les quatre racines de l'équation proposée.

On trouvera dans la Note V une nouvelle application remarquable de la méthode de Tschirnaüs.

NEUVIÈME LEÇON.

Développement d'une fonction algébrique implicite, en série ordonnée suivant les puissances décroissantes de sa variable. — Formation de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations à deux inconnues. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale. — Nouvelle démonstration d'une formule d'analyse. — Démonstration d'un théorème de géométrie.

Les recherches que je vais exposer dans cette leçon font partie d'un beau Mémoire sur l'élimination, publié par M. Liouville, dans le tome VI de son *Journal de Mathématiques*.

Développement d'une fonction algébrique implicite, en série ordonnée suivant les puissances décroissantes de sa variable.

Soit

$$(1) \qquad M(x, y) = 0, \quad \text{ou} \quad M = 0,$$

une équation du degré m entre deux variables x et y. Si cette équation est du degré m par rapport à y, elle aura m racines y, qui seront fonctions de x, et que nous nous proposons de développer suivant les puissances décroissantes de x. En réunissant les termes de même degré, l'équation (1) pourra s'écrire de la manière suivante :

$$(2) \qquad x^m f\left(\frac{y}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}\right) + x^{m-2} f_2\left(\frac{y}{x}\right) + \ldots = 0,$$

ou, en posant $\frac{y}{x} = u$,

$$(3) \qquad x^m f(u) + x^{m-1} f_1(u) + x^{m-2} f_2(u) + \ldots = 0;$$

f, f_1, f_2, etc., désignent ici des polynômes dont le premier est du degré m; les autres sont au plus des degrés $m-1$, $m-2$, etc., respectivement. Dans le cas le plus général, ces polynômes sont précisément des degrés m, $m-1$, $m-2$, etc.

Les m valeurs de u fournies par l'équation (3) sont des fonctions de x, qui, pour $x=\infty$, se réduiront aux m racines de l'équation

$$(4) \qquad f(\alpha)=0;$$

on pourra donc poser généralement

$$(5) \qquad u=\alpha+\varepsilon,$$

ε s'annulant avec $\frac{1}{x}$. La méthode des asymptotes donne le moyen de calculer la limite du produit εx. Nous nous bornerons au cas où les racines de l'équation (4) sont inégales, et dans tout ce qui suit, cette hypothèse doit être maintenue. Portons dans l'équation (3) la valeur de u tirée de (5); on aura

$$(6) \quad x^m f(\alpha+\varepsilon)+x^{m-1}f_1(\alpha+\varepsilon)+x^{m-2}f_2(\alpha+\varepsilon)+\ldots=0.$$

Développant chaque terme par la formule de Taylor, ayant égard à l'équation (4), et divisant par x^{m-1}, il vient

$$(7) \quad \left\{ \begin{array}{l} [(\varepsilon x)f'(\alpha)+f_1(\alpha)] \\ +\frac{1}{x}\left[\frac{(\varepsilon x)^2}{1.2}f''(\alpha)+(\varepsilon x)f'_1(\alpha)+f_2(\alpha)\right]+\ldots=0; \end{array} \right.$$

faisons maintenant $x=\infty$ dans cette équation, et désignant par α' la limite de εx, il vient

$$(8) \qquad \alpha' f'(\alpha)+f_1(\alpha)=0,$$

d'où

$$(9) \qquad \alpha'=-\frac{f_1(\alpha)}{f'(\alpha)}.$$

Cette valeur de α' sera toujours finie, car, par hypothèse, $f(\alpha)$ n'a pas de racines égales.

Puisque εx a pour limite la quantité α', dont nous venons de trouver la valeur, on pourra poser

$$\varepsilon x = \alpha' + \varepsilon',$$

d'où

$$(10) \qquad \varepsilon = \frac{\alpha'}{x} + \frac{\varepsilon'}{x},$$

ε' s'annulant avec $\frac{1}{x}$. Par suite, la valeur (5) de u devient

$$(11) \qquad u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x}.$$

C'est la série dans laquelle u se développe, quand on se borne aux deux premiers termes; $\frac{\varepsilon'}{x}$ est le reste correspondant.

On peut déterminer la limite du produit $\varepsilon' x$ de la même manière que celle du produit εx. Si, en effet, on porte dans l'équation (7) la valeur de ε, tirée de (10), qu'on multiplie ensuite par x, et qu'on ait égard à l'équation (8), il vient

$$(\varepsilon' x) f'(\alpha) + \left[\frac{\alpha'^2}{1.2} f''(\alpha) + \alpha' f'_1(\alpha) + f_2(\alpha)\right] + \mathrm{E} = 0,$$

en désignant par E une somme de termes qui s'annulent avec $\frac{1}{x}$; faisant donc $x = \infty$, et désignant par α'' la limite de $\varepsilon' x$, on a

$$(12) \quad \alpha'' f'(\alpha) + \left[\frac{\alpha'^2}{1.2} f''(\alpha) + \alpha' f'_1(\alpha) + f_2(\alpha)\right] = 0,$$

équation qui détermine la valeur de α''.

Connaissant la limite α'' du produit $\varepsilon' x$, on pourra poser

$$\varepsilon' x = \alpha'' + \varepsilon'';$$

d'où

(13) $$\varepsilon' = \frac{\alpha''}{x} + \frac{\varepsilon''}{x},$$

ε'' étant une nouvelle quantité qui s'évanouit avec $\frac{1}{x}$. D'après cela, la valeur (11) de u devient

(14) $$u = \alpha + \frac{\alpha'}{x} + \frac{\alpha''}{x^2} + \frac{\varepsilon''}{x^2}.$$

C'est la série qui exprime la valeur de u quand on se borne aux trois premiers termes; $\frac{\varepsilon''}{x^2}$ est le reste correspondant.

On pourra obtenir ainsi autant de termes que l'on voudra du développement de u, et comme $y = ux$, on aura, par suite, autant de termes que l'on voudra du développement de y; on a, en particulier,

(15) $$\begin{cases} y = \alpha x + \varepsilon x, \\ y = \alpha x + \alpha' + \varepsilon', \\ y = \alpha x + \alpha' + \dfrac{\alpha''}{x} + \dfrac{\varepsilon''}{x}. \end{cases}$$

La seconde de ces trois formules comprend toute la théorie des asymptotes rectilignes; la courbe représentée par l'équation (1), où x et y désignent alors des coordonnées rectilignes, a pour asymptote réelle ou imaginaire la droite représentée par l'équation

(16) $$y = \alpha x + \alpha'.$$

La différence ε' qui existe entre les coordonnées de la courbe et de l'asymptote est généralement un *infiniment petit du premier ordre*, en considérant $\frac{1}{x}$ lui-même comme un infiniment petit du premier ordre.

La courbe représentée par l'équation (1) admet aussi

pour asymptote l'hyperbole que représente l'équation

$$(17) \qquad y = \alpha x + \alpha' + \frac{\alpha''}{x};$$

mais dans ce cas la différence $\frac{\varepsilon''}{x}$ des ordonnées des deux courbes est un infiniment petit du second ordre au moins.

La courbe (17) pourrait être appelée *asymptote du deuxième ordre* de la courbe proposée. Et, comme on peut pousser aussi loin que l'on veut le développement de y en série ordonnée suivant les puissances décroissantes de x, on pourra former une infinité de courbes des degrés respectifs 3, 4, etc., et qui auront, avec la courbe proposée, un asymptotisme de plus en plus intime.

On voit aisément, sans qu'il soit nécessaire d'insister sur ce sujet, comment il faudrait modifier la méthode, si l'équation

$$f(\alpha) = 0$$

avait des racines égales, contrairement à l'hypothèse que nous avons faite.

Formation de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations à deux inconnues. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale.

La théorie qui vient d'être exposée permet de former autant de termes que l'on veut de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations. Soient les deux équations générales

$$(1) \qquad \begin{cases} M(x, y) = 0, \\ N(x, y) = 0, \end{cases}$$

des degrés m et n respectivement; en réunissant les termes de même degré, on pourra les écrire de la manière sui-

vante :

$$(2)\quad \begin{cases} x^m f\left(\frac{y}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}\right) + x^{m-2} f_2\left(\frac{y}{x}\right) + \ldots = 0, \\ x^n F\left(\frac{y}{x}\right) + x^{n-1} F_1\left(\frac{y}{x}\right) + x^{n-2} F_2\left(\frac{y}{x}\right) + \ldots = 0. \end{cases}$$

f, f_1, f_2, etc., sont des polynômes respectivement des degrés m, $m-1$, $m-2$, etc. ; F, F_1, F_2, etc., des polynômes des degrés n, $n-1$, $n-2$, etc.

Soient $y_1, y_2, \ldots, y_m$, les valeurs de y tirées de la première des équations (1), portons-les dans le premier membre de la seconde, et désignons par V le produit des résultats ainsi obtenus, de manière que l'on ait

$$(3)\qquad V = N(x, y_1)\,N(x, y_2)\ldots N(x, y_m);$$

l'équation finale qui résulte de l'élimination de y sera

$$V = 0.$$

On calculera aisément la fonction V, en développant en série suivant les puissances décroissantes de x, chacun de ses facteurs, dont l'expression générale est $N(x, y)$. Je dis même que, si l'on ne veut connaître que le premier terme de V, il suffit de borner les séries dont nous parlons à leur premier terme ; que, si l'on ne veut que les deux premiers termes de V, il suffit de connaître les deux premiers termes des séries, et ainsi de suite.

Supposons, par exemple, qu'on ne veuille connaître que le premier terme de V ; on a, en faisant comme précédemment $u = \frac{y}{x}$,

$$N(x, y) = x^n F(u) + x^{n-1} F_1(u) + \ldots.$$

Posons aussi, comme plus haut,

$$u = \alpha + \varepsilon,$$

ε étant une quantité qui s'annule avec $\frac{1}{x}$, et α une racine quelconque de l'équation

$$f(\alpha) = 0;$$

on aura

$$\frac{N(x, y)}{x^n} = F(\alpha + \varepsilon) + \frac{1}{x} F_1(\alpha + \varepsilon) + \ldots,$$

et pour $x = \infty$,

$$\lim \frac{N(x, y)}{x^n} = F(\alpha),$$

ou

$$(4) \qquad N(x, y) = x^n F(\alpha) + x^n E,$$

E désignant une quantité qui s'annule avec $\frac{1}{x}$. D'après cela, en représentant par

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

les m valeurs de α, on aura

$$N(x, y_1) = x^n F(\alpha_1) + x^n E_1,$$
$$N(x, y_2) = x^n F(\alpha_2) + x^n E_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$N(x, y_m) = x^n F(\alpha_m) + x^n E_m,$$

$E_1, E_2, \ldots, E_m$ désignant des quantités qui s'évanouissent avec $\frac{1}{x}$. Multipliant ces équations et ayant égard à l'équation (3), on aura

$$(5) \qquad V = x^{mn} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m) + x^{mn} H,$$

H désignant une quantité qui s'annule avec $\frac{1}{x}$.

Le premier terme de V est donc

$$x^{mn} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m);$$

on pourra l'exprimer en fonction rationnelle des coefficients de F et f, puisque $F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m)$ est une fonction symétrique et entière des racines de l'équation

$$f(\alpha) = 0.$$

Il suit de là que l'équation finale qui résulte de l'élimination de y entre les équations (1) et (2) est d'un degré égal au produit des degrés de ces équations.

Remarque. — Si les coefficients des équations (1) ont des valeurs déterminées, et que ces équations contiennent la plus haute puissance de y, l'équation finale résultant de l'élimination de y sera toujours $V = 0$, et l'on voit que le degré de cette équation finale sera encore égal au produit des degrés des équations proposées, à moins que les équations

$$f(\alpha) = 0, \quad F(\alpha) = 0$$

n'aient une ou plusieurs racines communes, auquel cas ce degré s'abaissera nécessairement.

Pour avoir les deux premiers termes de l'équation finale $V = 0$, il faut connaître les deux premiers termes du développement de $N(x, y)$ en série. Pour cela, dans l'équation

$$N(x, y) = x^n F(u) + x^{n-1} F_1(u) + \ldots,$$

nous poserons

$$u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x},$$

ε' désignant toujours une quantité qui s'évanouit avec $\frac{1}{x}$, α une racine de

$$f(\alpha) = 0,$$

et α' une quantité que nous avons calculée, et qui est déterminée par l'équation

$$\alpha' f'(\alpha) + f_1(\alpha) = 0;$$

on aura alors

$$N(x, y) = x^n F(\alpha) + x^{n-1}[\alpha' F'(\alpha) + F_1(\alpha)] + x^{n-1} E,$$

E désignant une quantité qui s'annule avec $\frac{1}{x}$. Cette formule donne le développement de $N(x, y)$, borné aux deux premiers termes; en y remplaçant α par chacune de ses m valeurs, on aura

$$N(x, y_1) = x^n F(\alpha_1) + x^{n-1}[\alpha'_1 F'(\alpha_1) + F_1(\alpha_1)] + x^{n-1} E_1,$$
$$N(x, y_2) = x^n F(\alpha_2) + x^{n-1}[\alpha'_2 F'(\alpha_2) + F_1(\alpha_2)] + x^{n-1} E_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$N(x, y_m) = x^n F(\alpha_m) + x^{n-1}[\alpha'_m F'(\alpha_m) + F_1(\alpha_m)] + x^{n-1} E_m.$$

Dans ces équations, E_1, E_2, etc., sont des quantités qui s'évanouissent avec $\frac{1}{x}$, et α'_1, α'_2, etc., sont les valeurs de α', qui correspondent aux valeurs α_1, α_2, etc., de α. Multipliant toutes ces équations et désignant simplement par $x^{mn-1} H$ l'ensemble des termes dont le quotient par x^{mn-1} s'annule avec $\frac{1}{x}$, on aura

$$V = x^{mn} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m)$$
$$+ x^{mn-1} F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m) \sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)} + x^{mn-1} H.$$

Dans cette dernière formule, la quantité H, qui est infiniment petite avec $\frac{1}{x}$, contient un nombre limité de termes, et l'on voit que le second terme de V aura pour coefficient

$$F(\alpha_1) F(\alpha_2) \ldots F(\alpha_m) \sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)},$$

le signe $\sum$ s'étendant à toutes les racines α de l'équation

$$f(\alpha) = 0.$$

D'après cela, si l'on désigne par $\sum x$ la somme des racines de l'équation finale en x, on aura

$$\sum x = -\sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)},$$

ou en mettant, au lieu de α', sa valeur $-\frac{f_1(\alpha)}{f'(\alpha)}$,

$$\sum x = \sum \frac{f_1(\alpha) F'(\alpha)}{f'(\alpha) F(\alpha)} - \sum \frac{F_1(\alpha)}{F(\alpha)}.$$

On pourrait calculer ainsi autant de termes que l'on voudrait de l'équation finale $V = o$; par suite, cette équation tout entière : seulement les calculs deviennent de plus en plus compliqués, et nous nous bornerons à ce qui précède.

Nouvelle démonstration d'une formule d'analyse.

Au lieu de porter dans l'équation $N = o$ les valeurs de y tirées de $M = o$, afin d'avoir l'équation finale $V = o$, on aurait pu faire l'inverse, porter dans l'équation $M = o$ les valeurs de y tirées de $N = o$; mais alors on aurait eu une autre expression de la somme $\sum x$ des racines de l'équation finale, que l'on peut écrire sans faire de nouveaux calculs. On aura, en effet, évidemment

$$\sum x = \sum \frac{F_1(6) f'(6)}{F'(6) f(6)} - \sum \frac{f_1(6)}{f(6)},$$

les sommes du second membre s'étendant à toutes les racines 6 de l'équation

$$F(6) = o;$$

en égalant entre elles ces deux valeurs de $\sum x$, on aura

$$\sum \frac{f_1(\alpha) F'(\alpha)}{f'(\alpha) F(\alpha)} - \sum \frac{F_1(\alpha)}{F(\alpha)} = \sum \frac{F_1(6) f'(6)}{F'(6) f(6)} - \sum \frac{f_1(6)}{f(6)},$$

les sommes du premier membre étant relatives aux racines α de $f(\alpha)=0$, celles du second aux racines 6 de $F(6)=0$. Dans cette formule, qui exprime un théorème d'analyse, f et F désignent des polynômes quelconques, mais n'ayant ni racines égales, ni racines communes; f_1 et F_1 désignent aussi des polynômes quelconques, mais de degrés respectivement moindres que f et F.

Supposons que le polynôme F soit égal à f_1, et que F_1 soit identiquement nul; l'équation précédente se réduit à

$$\sum \frac{F'(\alpha)}{f'(\alpha)} = -\sum \frac{F(6)}{f(6)},$$

ou même à

$$\sum \frac{F'(\alpha)}{f'(\alpha)} = 0,$$

puisque chaque terme du second membre est nul, le signe $\sum$ étant relatif aux racines de $F(6)=0$. Dans l'équation précédente, le signe $\sum$ s'étend aux racines α de $f(\alpha)=0$, et F' désigne la dérivée d'un polynôme quelconque F de degré inférieur à f; par conséquent, F' est un polynôme quelconque de degré inférieur à f'. La formule précédente est, comme nous l'avons vu, celle dont M. Liouville a déduit la décomposition des fractions rationnelles en fractions simples.

Démonstration d'un théorème de géométrie.

M. Liouville a déduit des résultats qui précèdent la démonstration d'un théorème curieux de géométrie; nous allons la présenter ici :

Si l'on mène à une courbe algébrique la série des tangentes parallèles à une direction donnée, le centre des

moyennes distances des points de contact sera indépendant de cette direction.

Soit

$$M(x, y) = 0$$

l'équation d'une courbe algébrique; les coordonnées réelles ou imaginaires des points de contact de cette courbe avec les tangentes parallèles à la droite $y = ax$ seront les solutions communes aux deux équations

$$(1) \qquad M = 0, \quad \frac{dM}{dx} + a\frac{dM}{dy} = 0.$$

Si l'on pose $\frac{y}{x} = u$, et qu'on représente la courbe par l'équation $\psi(x, u) = 0$, les coordonnées x et u seront les solutions communes aux deux équations

$$\varphi(x, u) = 0, \quad \frac{d\varphi}{dx} + \frac{a - u}{x}\frac{d\varphi}{du} = 0.$$

Soit donc, en conservant les notations employées précédemment,

$$\varphi(x, u) = x^m f(u) + x^{m-1} f_1(u) + \ldots,$$

f, f_1, etc., désignant des polynômes des degrés m, $m - 1$, etc.; on aura

$$\frac{d\varphi}{dx} = mx^{m-1} f(u) + (m-1)x^{m-2} f_1(u) + \ldots,$$

$$\frac{d\varphi}{du} = x^m f'(u) + x^{m-1} f_1'(u) + \ldots,$$

et, par suite,

$$\frac{d\varphi}{dx} + \frac{a-u}{x}\frac{d\varphi}{du} = x^{m-1} F(u) + x^{m-2} F_1(u) + \ldots,$$

en faisant, pour abréger,

$$(2) \qquad \begin{cases} F(u) = mf(u) + (a-u)f'(u), \\ F_1(u) = (m-1)f_1(u) + (a-u)f_1'(u), \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

$F(u)$, $F_1(u)$, etc., sont des polynômes des degrés $m-1$, $m-2$, etc.; car dans $F(u)$, par exemple, les deux termes du degré le plus élevé, qui proviennent de $mf(u)$ et de $(a-u)f'(u)$, se détruisent évidemment; et la même chose a lieu pour $F_1(u)$, etc.

L'équation finale résultant de l'élimination de y entre les équations (1) est donc la même que celle qui résulte de l'élimination de u entre

$$x^m f(u) + x^{m-1} f_1(u) + \ldots = 0,$$
$$x^{m-1} F(u) + x^{m-2} F_1(u) + \ldots = 0.$$

Si donc on désigne, comme précédemment, par $\sum x$ la somme des racines de l'équation finale, on aura

$$\sum x = -\sum \frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)},$$

le signe $\sum$ s'étendant dans le second membre aux racines de l'équation

$$f(\alpha) = 0,$$

et α' étant une quantité déterminée par l'équation

$$\alpha' f'(\alpha) + f_1(\alpha) = 0.$$

Pour avoir l'expression de $\sum x$ en fonction des quantités données f, f_1, etc., différentions la première des équations (2); on aura

$$(3) \qquad F'(u) = (m-1) f'(u) + (a-u) f''(u).$$

Les équations (2) et (3) donnent ensuite

$$\alpha' F'(\alpha) + F_1(\alpha) = (m-1)[\alpha' f'(\alpha) + f_1(\alpha)] + (a-\alpha)[\alpha' f''(\alpha) + f_1'(\alpha)],$$

et, comme $\alpha' f'(\alpha) + f_1(\alpha)$ est nul,

$$(4) \qquad \alpha' F'(\alpha) + F_1(\alpha) = (a-\alpha)[\alpha' f''(\alpha) + f_1'(\alpha)];$$

on aura aussi, en faisant $u = \alpha$ dans la première des équations (2), et remarquant que $f(\alpha)$ est nul,

$$(5) \qquad F(\alpha) = (a - \alpha) f'(\alpha).$$

Des équations (4) et (5) on tire

$$\frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)} = \frac{\alpha' f''(\alpha) + f'_1(\alpha)}{f'(\alpha)};$$

par suite, la valeur de $\sum x$ est

$$\sum x = - \sum \frac{\alpha' f''(\alpha) + f'_1(\alpha)}{f'(\alpha)}.$$

On voit qu'elle ne dépend pas de a. La somme des distances à l'axe des y des points de contact de notre courbe avec les tangentes parallèles à la direction donnée est donc indépendante de cette direction; ce qui démontre le théorème énoncé, car l'axe des y est une droite quelconque située dans le plan.

Remarque. — La démonstration précédente semble en défaut lorsque l'équation $f(\alpha) = 0$ a des racines égales; pour montrer que les conclusions sont cependant exactes dans ce cas, on peut employer un raisonnement dont nous avons déjà plusieurs fois fait usage. Il suffira de changer infiniment peu les coefficients de f, de manière que $f(\alpha) = 0$ n'ait plus de racines égales et de supposer ensuite ces changements nuls : on aura une courbe infiniment peu différente de la proposée, et pour laquelle le théorème aura lieu; d'où l'on peut conclure qu'il a lieu, à la limite, pour la courbe proposée elle-même.

Corollaire. — Désignons toujours par $\sum x$ la somme des abscisses des points de contact d'une courbe algébrique avec les tangentes qui font l'angle ω avec la direction des x positives, et faisons varier ω de sa différentielle $d\omega$;

comme $\sum x$ ne dépend pas de cet angle, on aura

$$\sum dx = 0.$$

Mais, en désignant par ds l'arc infiniment petit qui a pour projection dx, on a $dx = ds \cos \omega$; par suite,

$$\sum ds \cos \omega = 0, \quad \text{ou} \quad \sum \frac{ds}{d\omega} = 0,$$

puisque $\cos \omega$ et $d\omega$ sont constants. $\frac{ds}{d\omega}$ est la valeur du rayon de courbure ρ; on aura donc

$$\sum \rho = 0;$$

on aura aussi

$$\sum \frac{d\rho}{d\omega} = 0, \quad \text{ou} \quad \sum \rho' = 0,$$

ρ' désignant le rayon de courbure de la développée, et ainsi de suite.

En outre, si ξ et υ représentent les coordonnées du centre de courbure correspondant au point (x, y), on a

$$x = \xi - \rho \sin \omega, \quad y = \upsilon + \rho \cos \omega;$$

donc, en ayant égard aux formules précédentes,

$$\sum x = \sum \xi, \quad \sum y = \sum \upsilon;$$

c'est-à-dire que le centre des moyennes distances des points de contact d'une courbe algébrique avec la série des tangentes parallèles à une même direction, est le même que le centre des moyennes distances des centres de courbure correspondants.

DIXIÈME LEÇON.

Développement en séries ordonnées suivant les puissances décroissantes de la variabl, de plusieurs fonctions algébriques définies par autant d'équations. — Formation de l'équation finale qui résulte de l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale. — Démonstration d'une formule de M. Jacobi. — Extension du théorème de géométrie démontré dans la leçon précédente.

L'analyse que nous avons développée dans la dernière leçon peut être aisément généralisée, et étendue à l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. C'est ce que nous allons établir, en adoptant pour l'exposition le même ordre que dans la leçon précédente.

Développement en séries ordonnées suivant les puissances décroissantes de la variable, de plusieurs fonctions algébriques définies par autant d'équations.

Soient

$$(1) \qquad M(x, y, z) = 0, \quad N(x, y, z) = 0$$

deux équations générales des degrés m et n respectivement entre les trois variables x, y, z; la première x étant considérée comme indépendante, les deux autres y et z en seront des fonctions. En réunissant les termes de même degré, les équations (1) pourront s'écrire de la manière suivante :

$$(2) \qquad \begin{cases} x^m f\left(\dfrac{y}{x}, \dfrac{z}{x}\right) + x^{m-1} f_1\left(\dfrac{y}{x}, \dfrac{z}{x}\right) + \ldots = 0, \\ x^n F\left(\dfrac{y}{x}, \dfrac{z}{x}\right) + x^{n-1} F_1\left(\dfrac{y}{x}, \dfrac{z}{x}\right) + \ldots = 0, \end{cases}$$

ou, en posant $\frac{y}{x} = u$, $\frac{z}{x} = v$,

$$(3) \qquad \begin{cases} x^m f(u, v) + x^{m-1} f_1(u, v) + \ldots = 0, \\ x^n F(u, v) + x^{n-1} F_1(u, v) + \ldots = 0. \end{cases}$$

f et F sont des polynômes des degrés m et n respectivement, entre les variables u et v; f_1 et F_1 sont respectivement des degrés $m-1$ et $n-1$, et ainsi des autres.

En vertu des résultats obtenus dans la leçon précédente, le nombre des solutions communes (u, v) aux équations (3) est mn, ainsi que le nombre des solutions communes $(\alpha, 6)$ aux équations

$$(4) \qquad f(\alpha, 6) = 0, \quad F(\alpha, 6) = 0;$$

et les mn systèmes de solutions communes des équations (3) se réduiront, pour $x = \infty$, aux mn systèmes de solutions communes des équations (4). On pourra donc poser généralement

$$(5) \qquad u = \alpha + \varepsilon, \quad v = 6 + \eta,$$

ε et η désignant des quantités qui s'annulent avec $\frac{1}{x}$. Ces quantités sont d'ailleurs les restes des séries dans lesquelles u et v se développent quand on borne ces séries à leur premier terme. Pour calculer les limites des produits εx, ηx, nous suivrons la même marche que dans la leçon précédente. En portant dans les équations (3) les valeurs de u et v, tirées de (5), et ayant égard aux équations (4), on a

$$x^m\left(\varepsilon \frac{df}{d\alpha} + \eta \frac{df}{d6} + \ldots\right) + x^{m-1}[f_1(\alpha, 6) + \ldots] + \ldots = 0,$$

$$x^n\left(\varepsilon \frac{dF}{d\alpha} + \eta \frac{dF}{d6} + \ldots\right) + x^{n-1}[F_1(\alpha, 6) + \ldots] + \ldots = 0.$$

En divisant ces équations respectivement par x^{m-1} et

x^{n-1}, faisant ensuite $x = \infty$, et posant

$$\alpha' = \lim \varepsilon x, \quad \beta' = \lim \eta x,$$

on obtient

$$(6) \quad \begin{cases} \alpha' \dfrac{df}{d\alpha} + \beta' \dfrac{df}{d\beta} + f_1 = 0, \\ \alpha' \dfrac{dF}{d\alpha} + \beta' \dfrac{dF}{d\beta} + F_1 = 0, \end{cases}$$

d'où l'on tire les valeurs suivantes de α' et β' :

$$(7) \quad \begin{cases} \alpha' = \dfrac{F_1 \dfrac{df}{d\beta} - f_1 \dfrac{dF}{d\beta}}{\dfrac{df}{d\alpha}\dfrac{dF}{d\beta} - \dfrac{df}{d\beta}\dfrac{dF}{d\alpha}}, \\ \beta' = \dfrac{f_1 \dfrac{dF}{d\alpha} - F_1 \dfrac{df}{d\alpha}}{\dfrac{df}{d\alpha}\dfrac{dF}{d\beta} - \dfrac{df}{d\beta}\dfrac{dF}{d\alpha}}. \end{cases}$$

En désignant par ε' et η' de nouvelles quantités infiniment petites avec $\frac{1}{x}$, on pourra poser

$$\varepsilon x = \alpha' + \varepsilon', \quad \eta x = \beta' + \eta',$$

et, par suite,

$$u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x}, \quad v = \beta + \frac{\beta'}{x} + \frac{\eta'}{x};$$

on aura ainsi les deux premiers termes des séries dans lesquelles u et v, ou y et z peuvent se développer, et l'on voit aisément qu'on pourra, de la même manière, obtenir les termes suivants.

La même méthode s'appliquera, sans modification, au cas de $\mu - 1$ équations entre μ variables, pourvu qu'on écarte, comme nous l'avons fait jusqu'ici, en raisonnant sur des équations générales, quelques cas particuliers qui peuvent se présenter.

Formation de l'équation finale qui résulte de l'élimination de deux, trois, etc., inconnues entre trois, quatre, etc., équations. Nouvelle démonstration du théorème de Bezout. Somme des racines de l'équation finale.

On peut, par l'analyse précédente, former autant de termes que l'on veut, de l'équation finale qui résulte de l'élimination de deux, trois, etc., inconnues, entre trois, quatre, etc., équations.

Soient, par exemple, les trois équations générales

$$(1)\quad M(x, y, z) = 0, \quad N(x, y, z) = 0, \quad P(x, y, z) = 0,$$

des degrés m, n, p respectivement, entre trois inconnues x, y, z; en réunissant les termes de même degré, ces équations seront :

$$x^m f\left(\frac{y}{x}, \frac{z}{x}\right) + x^{m-1} f_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0,$$

$$x^n F\left(\frac{y}{x}, \frac{z}{x}\right) + x^{n-1} F_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0,$$

$$x^p \varphi\left(\frac{y}{x}, \frac{z}{x}\right) + x^{p-1} \varphi_1\left(\frac{y}{x}, \frac{z}{x}\right) + \ldots = 0.$$

f, F et φ sont des polynômes des degrés m, n, p respectivement, par rapport aux deux variables qu'ils renferment; f_1, F_1, φ_1 sont respectivement des degrés $m-1$, $n-1$, $p-1$, et ainsi de suite.

Désignons par

$$(y_1, z_1), \quad (y_2, z_2), \ldots, \quad (y_{mn}, z_{mn})$$

les mn systèmes de solutions communes aux deux premières des équations (1), et posons

$$V = P(x, y_1, z_1)\, P(x, y_2, z_2) \ldots P(x, y_{mn}, z_{mn});$$

l'équation finale résultant de l'élimination de y et z entre

les équations (1) sera

$$V = 0,$$

et c'est cette équation qu'il s'agit de calculer. On y parviendra en développant en série chacun des facteurs $P(x, y, z)$ de V, et il suffira de connaître autant de termes du développement de P qu'on en veut avoir dans V. Nous nous bornerons ici, comme nous l'avons fait dans la leçon précédente, à calculer les deux premiers termes de V, ce qui suffit pour connaître le degré et la somme des racines de l'équation finale.

On a, en faisant, comme précédemment, $\frac{y}{x} = u$, $\frac{z}{x} = v$,

$$P(x, y, z) = x^p \varphi(u, v) + x^{p-1} \varphi_1(u, v) + \ldots,$$

et, si l'on pose

$$u = \alpha + \varepsilon, \quad v = 6 + \eta,$$

il vient

$$P(x, y, z) = x^p \varphi(\alpha, 6) + x^p E,$$

E s'annulant avec $\frac{1}{x}$, ainsi que ε et η. En mettant dans l'équation précédente, à la place de x et y, leurs mn valeurs, il vient

$$P(x, y_1, z_1) = x^p \varphi(\alpha_1, 6_1) + x^p E_1,$$
$$P(x, y_2, z_2) = x^p \varphi(\alpha_2, 6_2) + x^p E_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$P(x, y_{mn}, z_{mn}) = x^p \varphi(\alpha_{mn}, 6_{mn}) + x^p E_{mn},$$

$E_1, E_2, \ldots, E_{mn}$ étant des quantités infiniment petites avec $\frac{1}{x}$. Enfin, en multipliant toutes ces équations, on a la valeur suivante de V,

$$V = x^{mnp} \varphi(\alpha_1, 6_1) \varphi(\alpha_2, 6_2) \ldots \varphi(\alpha_{mn}, 6_{mn}) + x^{mnp} H,$$

où H désigne une quantité qui s'annule avec $\frac{1}{x}$. Le pre-

mier terme de V est donc

$$x^{mnp}\varphi(\alpha_1, 6_1)\ldots\varphi(\alpha_{mn}, 6_{mn}).$$

Il suit de là que le degré de l'équation finale résultant de l'élimination de y et z entre les trois équations (1) est égal au produit des degrés de ces équations, ce qui fournit une nouvelle démonstration du théorème de Bezout.

Si l'on veut obtenir les deux premiers termes de l'équation finale $V = 0$, il est nécessaire de calculer les deux premiers termes du développement de $P(x, y, z)$ en série ordonnée suivant les puissances décroissantes de x. Pour cela, dans l'équation

$$P(x, y, z) = x^p\varphi(u, v) + x^{p-1}\varphi_1(u, v) + \ldots$$

nous poserons

$$u = \alpha + \frac{\alpha'}{x} + \frac{\varepsilon'}{x},$$

$$v = 6 + \frac{6'}{x} + \frac{\eta'}{x},$$

ε' et η' désignant toujours des quantités qui s'évanouissent avec $\frac{1}{x}$, α' et $6'$ des quantités déterminées par les équations

$$\alpha'\frac{df}{d\alpha} + 6'\frac{df}{d6} + f_1 = 0,$$

$$\alpha'\frac{dF}{d\alpha} + 6'\frac{dF}{d6} + F_1 = 0.$$

La valeur de $P(x, y, z)$ pourra alors s'écrire de la manière suivante :

$$P(x, y, z) = x^p\varphi(\alpha, 6)$$
$$+ x^{p-1}\left[\alpha'\frac{d\varphi}{d\alpha} + 6'\frac{d\varphi}{d6} + \varphi_1(\alpha, 6)\right] + x^{p-1}E,$$

en désignant par E une quantité qui s'annule avec $\frac{1}{x}$; on

aura donc

$$P(x, y_1, z_1) = x^p \varphi(\alpha_1, \text{β}_1)$$

$$+ x^{p-1}\left[\alpha'_1 \frac{d\varphi}{d\alpha_1} + \text{β}'_1 \frac{d\varphi}{d\text{β}_1} + \varphi_1(\alpha_1, \text{β}_1)\right] + x^{p-1} E_1,$$

. . . .

. . . .

$$P(x, y_{mn}, z_{mn}) = x^p \varphi(\alpha_{mn}, \text{β}_{mn})$$

$$+ x^{p-1}\left[\alpha'_{mn} \frac{d\varphi}{d\alpha_{mn}} + \text{β}'_{mn} \frac{d\varphi}{d\text{β}_{mn}} + \varphi_1(\alpha_{mn}, \text{β}_{mn})\right] + x^{p-1} E_{mn}.$$

Dans ces équations nous avons mis, pour abréger, $\frac{d\varphi}{d\alpha_1}$, etc., à la place de $\frac{d\varphi(\alpha_1, \text{β}_1)}{d\alpha_1}$, etc.; α'_1, α'_2, etc., désignent les valeurs de α' qui correspondent aux valeurs α_1, α_2, etc., de α; enfin, E_1, E_2, etc., sont des quantités infiniment petites avec $\frac{1}{x}$. En multipliant toutes ces équations, on aura la valeur suivante de V :

$$V = x^{mnp} \varphi(\alpha_1, \text{β}_1)\varphi(\alpha_2, \text{β}_2)\ldots\varphi(\alpha_{mn}, \text{β}_{mn})$$

$$+ x^{mnp-1} \varphi(\alpha_1, \text{β}_1)\ldots\varphi(\alpha_{mn}, \text{β}_{mn}) \sum \frac{\alpha' \frac{d\varphi}{d\alpha} + \text{β}' \frac{d\varphi}{d\text{β}} + \varphi_1(\alpha, \text{β})}{\varphi(\alpha, \text{β})}$$

$$+ x^{mnp-1} H,$$

où H désigne une quantité qui s'annule avec $\frac{1}{x}$, et où le signe $\sum$ s'étend à toutes les solutions communes $(\alpha, \text{β})$, des deux équations

$$f(\alpha, \text{β}) = 0, \quad F(\alpha, \text{β}) = 0.$$

Le second terme de V est donc

$$x^{mnp-1} \varphi(\alpha_1, \text{β}_1)\ldots\varphi(\alpha_{mn}, \text{β}_{mn}) \sum \frac{\alpha' \frac{d\varphi}{d\alpha} + \text{β}' \frac{d\varphi}{d\text{β}} + \varphi_1}{\varphi};$$

et si l'on désigne par $\sum x$ la somme des racines de l'équation finale $V = 0$, on aura

$$\sum x = -\sum \frac{\alpha' \frac{d\varphi}{d\alpha} + 6' \frac{d\varphi}{d6} + \varphi_1}{\varphi}.$$

En remplaçant, dans cette formule, α' et $6'$ par leurs valeurs écrites plus haut, et faisant, pour abréger,

$$A(\alpha, 6) = \frac{dF}{d\alpha}\frac{d\varphi}{d6} - \frac{d\varphi}{d\alpha}\frac{dF}{d6},$$

$$B(\alpha, 6) = \frac{d\varphi}{d\alpha}\frac{df}{d6} - \frac{df}{d\alpha}\frac{d\varphi}{d6},$$

$$C(\alpha, 6) = \frac{df}{d\alpha}\frac{dF}{d6} - \frac{dF}{d\alpha}\frac{df}{d6},$$

on aura cette expression

$$\sum x = -\sum \frac{\varphi_1(\alpha, 6)}{\varphi(\alpha, 6)} - \sum \frac{f_1(\alpha, 6)A(\alpha, 6) + F_1(\alpha, 6)B(\alpha, 6)}{\varphi(\alpha, 6)C(\alpha, 6)},$$

où les sommes du second membre sont relatives à tous les couples de solutions communes aux deux équations

$$f(\alpha, 6) = 0, \quad F(\alpha, 6) = 0.$$

Le calcul des deux premiers termes de l'équation finale, qui résulterait de l'élimination de $\mu - 1$ inconnues entre μ équations, n'offrira pas plus de difficulté, quel que soit μ, que dans les deux cas particuliers que nous avons développés; la marche à suivre est toujours la même, et l'on peut considérer comme générale la nouvelle démonstration que nous avons donnée du théorème de Bezout pour le cas de deux ou trois équations.

Démonstration d'une formule de M. Jacobi.

Pour obtenir l'équation finale $V = 0$, nous avons porté

dans la troisième des équations données les valeurs de y et z, tirées des deux premières; mais on aurait pu opérer de deux autres manières différentes : on aurait pu, par exemple, porter dans la première, les valeurs de y et z, tirées des deux dernières, et l'on aurait obtenu une expression différente de $\sum x$, qui se déduirait évidemment de celle déjà trouvée, en changeant l'une en l'autre f et φ, f_1 et φ_1, etc. On aura donc

$$\sum x = -\sum \frac{f_1(\gamma, \delta)}{f(\gamma, \delta)} - \sum \frac{F_1(\gamma, \delta)\, B(\gamma, \delta) + \varphi_1(\gamma, \delta)\, C(\gamma, \delta)}{f(\gamma, \delta)\, A(\gamma, \delta)};$$

mais ici les sommes qui figurent dans le second membre sont relatives aux solutions communes des équations

$$F(\gamma, \delta) = 0, \quad \varphi(\gamma, \delta) = 0.$$

Égalons les deux valeurs trouvées pour $\sum x$, et supposons que les polynômes F_1 et f_1 soient identiquement nuls; on aura

$$\sum \frac{\varphi_1(\alpha, 6)}{\varphi(\alpha, 6)} = \sum \frac{\varphi_1(\gamma, \delta)\, C(\gamma, \delta)}{f(\gamma, \delta)\, A(\gamma, \delta)},$$

en se rappelant que le signe $\sum$ s'étend, dans le premier membre, aux solutions communes de $f(\alpha, 6) = 0$, $F(\alpha, \beta) = 0$, et, dans le second membre, aux solutions communes de $F(\gamma, \delta) = 0$, $\varphi(\gamma, \delta) = 0$. On peut, dans cette formule, considérer les polynômes f, F et φ comme absolument arbitraires; et, quant au polynôme φ_1, il n'est assujetti, par notre analyse, qu'à la seule condition d'être de degré inférieur à φ. Supposons

$$\varphi(\alpha, 6) = C(\alpha, 6);$$

la somme du second membre de l'équation précédente sera alors relative aux solutions communes des deux

équations

$$F(\gamma, \delta) = 0, \quad C(\gamma, \delta) = 0,$$

et, par conséquent, chacun de ses termes sera identiquement nul. On aura donc

$$\sum \frac{\varphi_1(\alpha, 6)}{C(\alpha, 6)} = 0$$

ou

$$\sum \frac{\varphi_1(\alpha, 6)}{\frac{df}{d\alpha}\frac{dF}{d\beta} - \frac{dF}{d\alpha}\frac{df}{d\beta}} = 0,$$

le signe $\sum$ s'étendant aux solutions communes des deux équations

$$f(\alpha, 6) = 0, \quad F(\alpha, 6) = 0.$$

Cette formule curieuse, où φ_1 désigne un polynôme quelconque de degré inférieur à celui de $\frac{df}{d\alpha}\frac{dF}{d\beta} - \frac{dF}{d\alpha}\frac{df}{d\beta}$, est l'extension de celle que nous avons démontrée dans la cinquième leçon, et à laquelle nous avons été de nouveau conduit dans la leçon précédente. Elle a été démontrée pour la première fois par M. Jacobi, et M. Liouville l'a trouvée, ainsi que nous venons de le faire voir, comme une conséquence naturelle de ses recherches sur l'élimination.

Extension du théorème de géométrie démontré dans la leçon précédente.

M. Liouville a donné dans son Mémoire la démonstration du théorème suivant, qui est l'extension de celui que nous avons établi dans la dernière leçon :

Théorème. — *Si l'on mène à une surface algébrique la série des plans tangents parallèles à deux directions*

fixes, le centre des moyennes distances des points de contact sera indépendant de ces deux directions.

Si

$$M(x, y, z) = o$$

est l'équation d'une surface algébrique, les coordonnées des points de contact de cette surface avec les plans tangents parallèles au plan qui a pour équations

$$z = ax + by,$$

seront données par les trois équations

$$M = o, \quad \frac{dM}{dx} + a\frac{dM}{dz} = o, \quad \frac{dM}{dy} + b\frac{dM}{dz} = o.$$

Il suffit, pour établir le théorème qui vient d'être énoncé, de calculer la somme des racines de l'équation finale qui résulte de l'élimination de deux inconnues entre les trois équations précédentes. En suivant la marche que nous avons tracée, on trouvera que cette somme est indépendante de a et de b. Ce calcul ne présentant aucune difficulté, nous nous dispenserons de le présenter ici, et nous renverrons, pour plus de détails, au Mémoire de M. Liouville. On y trouvera, du reste, un grand nombre de conséquences curieuses que nous ne pourrions développer sans sortir de limites que nous nous sommes imposées.

ONZIÈME LEÇON.

Théorème sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. — Des fonctions semblables. — Propriétés des fonctions semblables des racines d'une équation. — Examen des cas particuliers qui font exception. — Méthode pour calculer une fonction des racines d'une équation, quand on connaît une autre fonction quelconque des racines.

Parmi les travaux publiés depuis un siècle sur la théorie algébrique des équations, l'un des plus importants est, sans contredit, le célèbre Mémoire de Lagrange, que nous avons déjà eu l'occasion de citer, et qui fait partie des *Mémoires de l'Académie de Berlin* pour 1770 et 1771. On rencontre, entre autres résultats remarquables, dans ce grand travail, le beau théorème que voici :

Dès qu'on aura trouvé, par un moyen quelconque, la valeur d'une fonction rationnelle des racines d'une équation, on pourra, en général, trouver la valeur d'une autre fonction rationnelle quelconque des mêmes racines, et cela par le moyen d'une équation simplement linéaire. Quelques cas particuliers exigeront la résolution d'une équation du deuxième, du troisième, etc., degré.

La démonstration de ce théorème et le développement de ses conséquences feront le sujet de cette leçon ; mais, pour ne pas interrompre notre exposition, nous commencerons par établir une proposition importante, dont nous aurons besoin.

Théorème sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme.

Soit

$$V = F(a, b, c, \ldots, k, l)$$

une fonction de m lettres $a, b, c, \ldots, k, l$.

Désignons, pour abréger,

$$A_1, A_2, A_3, \ldots, A_M$$

les $M = 1.2\ldots m$ permutations dont ces lettres sont susceptibles, et représentons par la notation

$$\begin{pmatrix} A_\alpha \\ A_\beta \end{pmatrix}$$

l'opération qui consiste à remplacer les lettres de la permutation A_α par celles de même rang dans la permutation A_β : cette opération se nomme une *substitution*.

On obtiendra toutes les valeurs que la fonction V peut prendre par les permutations des lettres a, b, c, etc., en lui appliquant les M substitutions

$$\begin{pmatrix} A_1 \\ A_1 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, \begin{pmatrix} A_1 \\ A_3 \end{pmatrix}, \ldots, \begin{pmatrix} A_1 \\ A_M \end{pmatrix},$$

dont la première est une substitution *identique;* il en résultera, pour la fonction V, M valeurs que nous désignerons par

$$V_1, V_2, \ldots, V_M.$$

On voit que le nombre des valeurs distinctes de V est au plus égal à M : mais il peut être moindre; cela arrivera, par exemple, si la fonction V est symétrique par rapport à quelques-unes des m lettres a, b, etc.

Il peut arriver aussi qu'une fonction qui n'est symé-

trique par rapport à aucunes lettres, ne puisse pas cependant acquérir M valeurs distinctes. Nous citerons pour exemple la fonction

$$(a-b)(a-c)(b-c),$$

qui ne peut acquérir que deux valeurs, bien qu'elle ne soit pas symétrique par rapport à deux des trois lettres qu'elle renferme.

Quand nous disons qu'une substitution change ou ne change pas la valeur d'une fonction, il est bien entendu que nous faisons abstraction des valeurs numériques qu'on peut, ultérieurement, attribuer aux lettres, et que nous ne voulons parler que de la *valeur algébrique* de la fonction. Ainsi la fonction

$$a+2b+3c$$

est changée par la substitution $\begin{pmatrix} a, & b, & c \\ b, & c, & a \end{pmatrix}$, quoique la nouvelle valeur qu'elle prend, savoir,

$$b+2c+3a,$$

puisse être égale à la première, si l'on attribue des valeurs convenables aux lettres a, b, c.

Théorème. — *Le nombre des valeurs distinctes que peut prendre une fonction de m lettres, quand on y permute les lettres qu'elle renferme, est toujours un diviseur du produit* $1.2.3...m$.

Supposons que les valeurs de la fonction V,

$$(1) \qquad V_1,\ V_2,\ldots,\ V_M,$$

formées comme il vient d'être dit, ne soient pas toutes distinctes, et que le nombre de celles qui sont égales à V_α, par exemple, soit n; que l'on ait, par conséquent, ces n valeurs égales

$$(2) \qquad V_\alpha = V_\beta = V_\gamma = \ldots = V_\omega,$$

qui correspondent respectivement aux permutations

(3) $$A_\alpha,\ A_\beta,\ A_\gamma,\ldots,\ A_\omega,$$

ou, en d'autres termes, qui se déduisent de V_1 par les substitutions

$$\begin{pmatrix}A_1\\A_\alpha\end{pmatrix},\quad \begin{pmatrix}A_1\\A_\beta\end{pmatrix},\quad \begin{pmatrix}A_1\\A_\gamma\end{pmatrix},\ldots,\quad \begin{pmatrix}A_1\\A_\omega\end{pmatrix}.$$

Soient $V_{\alpha'}$ l'une des fonctions (1) qui ne sont pas égales à V_α, $A_{\alpha'}$ la permutation correspondante, en sorte que $V_{\alpha'}$ se déduise de V_1 par la substitution $\begin{pmatrix}A_1\\A_{\alpha'}\end{pmatrix}$, et considérons les n permutations

(4) $$A_{\alpha'},\ A_{\beta'},\ A_{\gamma'},\ldots,\ A_{\omega'},$$

formées de telle sorte que $A_{\beta'}$, $A_{\gamma'}$, etc., se déduisent de $A_{\alpha'}$, de la même manière que A_β, A_γ, etc., se déduisent de A_α, c'est-à-dire en exécutant les mêmes changements entre les lettres qui occupent les mêmes places. Par exemple, si A_β se déduit de A_α en remplaçant dans A_α les lettres qui occupent les rangs 1, 2, 3, 4, respectivement par celles qui occupent les rangs 2, 4, 1, 3, de même aussi $A_{\beta'}$ devra être formée en remplaçant les lettres qui occupent dans $A_{\alpha'}$ les rangs 1, 2, 3, 4, respectivement par celles qui occupent les rangs 2, 4, 1, 3.

Soient aussi

(5) $$V_{\alpha'},\ V_{\beta'},\ V_{\gamma'},\ldots,\ V_{\omega'}$$

les valeurs de V en nombre égal à n, et qui correspondent aux permutations (4); c'est-à-dire qu'on déduit de V_1 par les substitutions

$$\begin{pmatrix}A_1\\A_{\alpha'}\end{pmatrix},\quad \begin{pmatrix}A_1\\A_{\beta'}\end{pmatrix},\quad \begin{pmatrix}A_1\\A_{\gamma'}\end{pmatrix},\ldots,\quad \begin{pmatrix}A_1\\A_{\omega'}\end{pmatrix}.$$

Je dis que les égalités (2) entraîneront nécessairement les suivantes :

$$V_{\alpha'} = V_{\beta'} = V_{\gamma'} = \ldots = V_{\omega'}.$$

En effet, V_α et V_β se déduisant de V_1 par les substitutions $\begin{pmatrix} A_1 \\ A_\alpha \end{pmatrix}$, $\begin{pmatrix} A_1 \\ A_\beta \end{pmatrix}$, il est évident que V_β se déduira de V_α par la substitution $\begin{pmatrix} A_\alpha \\ A_\beta \end{pmatrix}$; pareillement, $V_{\beta'}$ se déduira de $V_{\alpha'}$ en appliquant à cette dernière la substitution $\begin{pmatrix} A_{\alpha'} \\ A_{\beta'} \end{pmatrix}$. Or, par hypothèse, la substitution $\begin{pmatrix} A_\alpha \\ A_\beta \end{pmatrix}$ ne produit aucun changement sur V_α, donc la substitution $\begin{pmatrix} A_{\alpha'} \\ A_{\beta'} \end{pmatrix}$ ne produira aucun changement sur $V_{\alpha'}$, car $V_{\alpha'}$, $A_{\alpha'}$, $A_{\beta'}$ ne sont autre chose que V_α, A_α, A_β où l'on a changé la *notation* d'une certaine manière. On a donc $V_{\alpha'} = V_{\beta'}$, et l'on voit que, pour la même raison, les fonctions (5) seront toutes égales entre elles. D'ailleurs les n fonctions (5) correspondent respectivement aux permutations (4), qui sont évidemment distinctes et différentes des permutations (3); donc elles se trouveront parmi les M fonctions (1), et l'on aura, par suite,

$$M = 2n \quad \text{ou} \quad M > 2n.$$

Si $M > 2n$ et que $V_{\alpha''}$ désigne l'une des valeurs de V distinctes de V_α et de $V_{\alpha'}$, on fera voir, comme précédemment, que la série (1) contient n nouveaux termes

$$V_{\alpha''},\ V_{\beta''},\ V_{\gamma''}, \ldots,\ V_{\omega''},$$

tous égaux entre eux : on aura, par conséquent,

$$M = 3n \quad \text{ou} \quad M > 3n;$$

et, en poursuivant ce raisonnement, on voit que les M

fonctions de la série (1) se partageront nécessairement en un certain nombre μ de groupes composés chacun de n fonctions égales entre elles : on aura donc

$$M = \mu n, \quad \text{d'où} \quad \mu = \frac{M}{n};$$

le nombre μ des valeurs distinctes de V est donc un diviseur du produit $M = 1.2.3\ldots m$, comme nous l'avions annoncé.

Ce théorème a été démontré, pour la première fois, par Lagrange, dans le Mémoire cité plus haut. Nous avons suivi, dans la démonstration précédente, la marche indiquée par M. Cauchy dans son Mémoire *sur le nombre des valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme*, Mémoire qui fait partie du tome X du *Journal de l'École Polytechnique*.

Des fonctions semblables.

Deux fonctions de m quantités sont dites *semblables* lorsque les substitutions qui changent la valeur de l'une changent aussi la valeur de l'autre, ou, ce qui revient au même, lorsque les substitutions qui laissent l'une d'elles invariable ne produisent non plus aucun changement sur l'autre.

Ainsi, deux fonctions symétriques des m racines d'une équation sont deux fonctions semblables qui ne peuvent prendre chacune qu'une seule valeur; et, plus généralement, si

$$x_1, x_2, \ldots, x_m$$

désignent les m racines d'une équation de degré m, deux fonctions symétriques de n d'entre elles,

$$x_1, x_2, \ldots, x_n$$

par exemple, seront aussi deux fonctions semblables des

m racines, et chacune d'elles pourra acquérir un nombre de valeurs égal au nombre des combinaisons de m lettres n à n, c'est-à-dire égal à

$$\frac{m(m-1)\ldots(m-n+1)}{1.2\ldots n}.$$

Nous ne considérons ici que des fonctions rationnelles.

Propriété des fonctions semblables des racines d'une équation.

Deux fonctions semblables des racines d'une équation sont exprimables rationnellement l'une par l'autre, en sorte que si l'on connaît la valeur d'une fonction quelconque des racines, on pourra déterminer la valeur de toutes les fonctions semblables.

Il y a pourtant quelques cas d'exception que nous examinerons en détail.

Soient, en effet,

$$x_1,\ x_2,\ldots,\ x_m$$

les m racines de l'équation

(1) $$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

et

$$V = F(x_1, x_2, \ldots, x_m),$$
$$y = f(x_1, x_2, \ldots, x_m),$$

deux fonctions rationnelles et semblables de ces racines dont la première est supposée avoir une valeur connue.

Appliquons simultanément, aux fonctions F et f, toutes les $1.2.3\ldots m$ substitutions possibles; il en résultera pour V un certain nombre μ de valeurs distinctes, que je représente par

(2) $$V_1,\ V_2,\ldots,\ V_\mu,$$

et pour la fonction semblable y, les μ valeurs correspondantes

(3) $$y_1, y_2, \ldots, y_\mu.$$

On peut former, par la méthode indiquée dans la troisième leçon, l'équation qui a pour racines les μ valeurs de V : soit

(4) $$V^\mu + P_1 V^{\mu-1} + P_2 V^{\mu-2} + \ldots + P_{\mu-1} V + P_\mu = 0,$$

ou

$$\psi(V) = 0,$$

cette équation, dont les coefficients sont exprimables rationnellement par ceux de l'équation proposée. On pourrait former, de la même manière, l'équation qui a pour racines les μ valeurs de y; mais cette équation ne nous sera pas nécessaire.

Considérons maintenant la fonction

$$V^n y,$$

où n est un nombre entier quelconque; les valeurs que peut prendre cette fonction par les diverses substitutions seront évidemment

$$V_1^n y_1, \quad V_2^n y_2, \quad V_3^n y_3, \ldots, \quad V_\mu^n y_\mu,$$

puisque, généralement, toute substitution qui change V en V_ρ change aussi y en y_ρ, et il suit de là (troisième leçon) que la quantité

$$V_1^n y_1 + V_2^n y_2 + V_3^n y_3 + \ldots + V_\mu^n y_\mu$$

sera une fonction symétrique des m racines $x_1, x_2, \ldots, x_m$, et qu'elle pourra, par conséquent, s'exprimer rationnellement en fonction des coefficients p_1, p_2, etc., de l'é-

quation (1), quel que soit l'entier n. Donnons à n les valeurs successives $0, 1, 2, \ldots, (\mu - 1)$, et posons

$$(5)\begin{cases} y_1 + y_2 + y_3 + \ldots + y_\mu = t_0, \\ V_1 y_1 + V_2 y_2 + V_3 y_3 + \ldots + V_\mu y_\mu = t_1, \\ V_1^2 y_1 + V_2^2 y_2 + V_3^2 y_3 + \ldots + V_\mu^2 y_\mu = t_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ V_1^{\mu-1} y_1 + V_2^{\mu-1} y_2 + V_3^{\mu-1} y_3 + \ldots + V_\mu^{\mu-1} y_\mu = t_{\mu-1}. \end{cases}$$

Les seconds membres t_0, t_1, etc., de ces équations sont tous exprimables rationnellement en fonction des coefficients de l'équation proposée et des quantités connues qui entrent dans F et f; on peut donc les considérer comme connus, et si l'on résout les μ équations (5) par rapport à $y_1, y_2, \ldots, y_\mu$, chacune de ces valeurs de y se trouvera exprimée, comme on va voir, en fonction rationnelle de la valeur correspondante de V.

Ajoutons les équations (5), après les avoir multipliées respectivement par les facteurs

$$\lambda_0,\ \lambda_1,\ \lambda_2, \ldots,\ \lambda_{\mu-2},\ 1,$$

et faisons, pour abréger,

$$(6)\qquad \varphi(V) = V^{\mu-1} + \lambda_{\mu-2} V^{\mu-2} + \ldots + \lambda_1 V + \lambda_0,$$

on aura

$$(7)\qquad \begin{cases} y_1 \varphi(V_1) + y_2 \varphi(V_2) + \ldots + y_\mu \varphi(V_\mu) \\ = t_0 \lambda_0 + t_1 \lambda_1 + \ldots + t_{\mu-1} \lambda_{\mu-2} + t_{\mu-1}, \end{cases}$$

et si l'on veut la valeur de y_ρ par exemple, il suffira de déterminer les facteurs λ_0, λ_1, etc., de manière que l'on ait

$$(8)\qquad \varphi(V_1) = 0,\quad \varphi(V_2) = 0, \ldots,\quad \varphi(V_\mu) = 0,$$

excepté $\varphi(V_\rho) = 0$; alors l'équation (7) donnera

$$(9) \qquad y_\rho = \frac{t_0\lambda_0 + t_1\lambda_1 + \ldots + t_{\mu-2}\lambda_{\mu-2} + t_{\mu-1}}{\varphi(V_\rho)},$$

et il ne reste plus qu'à trouver les valeurs de λ_0, λ_1, etc.; ce que l'on peut faire très-aisément de la manière suivante.

Les équations (8) qui déterminent ces facteurs expriment que l'équation

$$\varphi(V) = 0$$

a pour racines $V_1, V_2, \ldots, V_\mu$, excepté V_ρ; mais l'équation (4)

$$\psi(V) = 0$$

a ces mêmes racines, y compris V_ρ; et comme d'ailleurs les plus hautes puissances de V dans $\varphi(V)$ et dans $\psi(V)$ ont pour coefficient l'unité, on aura identiquement

$$\varphi(V) = \frac{\psi(V)}{V - V_\rho},$$

ou, en développant le quotient de $\psi(V)$ par $V - V_\rho$,

$$\varphi(V) = V^{\mu-1} + \left.\begin{matrix} P_1 \\ + V_\rho \end{matrix}\right| V^{\mu-2} + \left.\begin{matrix} P_2 \\ + P_1 V_\rho \\ + V_\rho^2 \end{matrix}\right| V^{\mu-3} + \ldots + \begin{matrix} P_{\mu-1} \\ + P_{\mu-2} \\ + P_{\mu-3} V_\rho^2 \\ \vdots \\ + P_1 V_\rho^{\mu-2} \\ + V_\rho^{\mu-1}. \end{matrix}$$

En identifiant cette valeur de $\varphi(V)$ avec celle donnée par l'équation (6), on obtient les valeurs suivantes des fac-

teurs λ :

$$(10)\quad \left\{\begin{array}{l} \lambda_{\mu-2} = P_1 + V_\rho, \\ \lambda_{\mu-3} = P_2 + P_1 V_\rho + V_\rho^2, \\ \lambda_{\mu-4} = P_3 + P_2 V_\rho + P_1 V_\rho^2 + V_\rho^3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \lambda_0 \ldots = P_{\mu-1} + P_{\mu-2} V_\rho + \ldots + P_1 V_\rho^{\mu-2} + V_\rho^{\mu-1}. \end{array}\right.$$

Ces facteurs étant tous exprimés en fonction de V_ρ et des quantités connues, il en sera de même de y_ρ. On peut donner à l'expression de y_ρ une forme très-simple.

En faisant, pour abréger l'écriture,

$$\begin{array}{l} T_{\mu-1} = t_{\mu-1} + P_1 t_{\mu-2} + P_2 t_{\mu-3} + \ldots + P_{\mu-2} t_1 + P_{\mu-1} t_0, \\ T_{\mu-2} = t_{\mu-2} + P_1 t_{\mu-3} + P_2 t_{\mu-4} + \ldots + P_{\mu-2} t_0, \\ T_{\mu-3} = t_{\mu-3} + P_1 t_{\mu-4} + \ldots\ldots + P_{\mu-3} t_0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ T_1 = t_1 + P_1 t_0, \\ T_0 = t_0, \end{array}$$

le numérateur de la valeur de y_ρ, donnée par l'équation (9), sera

$$T_0 V_\rho^{\mu-1} + T_1 V_\rho^{\mu-2} + \ldots + T_{\mu-2} V_\rho + T_{\mu-1};$$

et quant au dénominateur, il est égal à $\varphi(V_\rho)$, c'est-à-dire à la valeur que prend la fraction $\frac{\psi(V)}{V - V_\rho}$ pour $V = V_\rho$: cette valeur est $\psi'(V_\rho)$, ψ' désignant la dérivée de ψ. Or,

$$\psi'(V) = \mu V^{\mu-1} + (\mu - 1) P_1 V^{\mu-2} + \ldots + P_{\mu-1};$$

on aura donc la valeur suivante de y_ρ :

$$(11)\quad y_\rho = \frac{T_0 V_\rho^{\mu-1} + T_1 V_\rho^{\mu-2} + \ldots + T_{\mu-2} V_\rho + P_{\mu-1}}{\mu V_\rho^{\mu-1} + (\mu-1) P_1 V_\rho^{\mu-2} + \ldots + 2 P_{\mu-2} V_\rho + P_{\mu-1}},$$

ou, en désignant simplement par V l'une quelconque des valeurs V_1, V_2, etc., par y la valeur correspondante de y,

$$(12)\quad y = \frac{T_0 V^{\mu-1} + T_1 V^{\mu-2} + \ldots + T_{\mu-2} V + T_{\mu-1}}{\mu V^{\mu-1} + (\mu-1) P_1 V^{\mu-2} + \ldots + 2 P_{\mu-2} V + P_{\mu-1}},$$

valeur que nous représenterons aussi, pour abréger, par

$$y = \frac{\Theta(V)}{\psi'(V)}.$$

Examen des cas particuliers qui font exception.

D'après ce qui précède, les valeurs de $y_1, y_2, \ldots, y_\mu$ s'exprimeront rationnellement en fonction de $V_1, V_2, \ldots, V_\mu$, respectivement par les formules

$$(13)\quad y_1 = \frac{\Theta(V_1)}{\psi'(V)}, \quad y_2 = \frac{\Theta(V_2)}{\psi'(V_2)}, \ldots, \quad y_\mu = \frac{\Theta(V_\mu)}{\psi'(V_\mu)}.$$

Mais quelques-unes de ces équations seront illusoires si l'équation

$$\psi(V) = 0$$

a des racines égales; elles le seront même toutes si la précédente équation en V n'a que des racines multiples. Toutefois, si V_ρ est une racine simple de l'équation en V, la valeur correspondante y_ρ sera, dans tous les cas, donnée par la formule

$$y_\rho = \frac{\Theta(V_\rho)}{\psi'(V_\rho)}.$$

Les cas d'exception que nous venons de signaler peuvent évidemment se présenter; car, bien que les fonctions

$$V_1,\ V_2,\ldots,\ V_\mu$$

soient distinctes, quant à la forme algébrique, si les quantités x_1, x_2, etc., dont elles dépendent, ont des valeurs déterminées, quelques-unes de ces fonctions peuvent être *numériquement* égales. Alors les équations (5) sont insuffisantes pour déterminer y_1, y_2, etc.

Supposons, par exemple, que $V_2=V_1$, mais que toutes les autres valeurs de V soient différentes et distinctes de V_1 : les inconnues y_1 et y_2 n'entreront dans les équations (5) que combinées entre elles par voie d'addition, et ces équations (5) ne pourront déterminer que

$$(y_1+y_2),\ y_3,\ y_4,\ldots,\ y_\mu,$$

qui sont au nombre de $\mu-1$; l'une des équations (5) deviendra inutile, et, en se bornant aux $\mu-1$ premières, on aura

$$\begin{aligned}
(y_1+y_2)+y_3+y_4+\ldots+y_\mu&=t_0,\\
V_1(y_1+y_2)+V_3y_3+\ldots+V_\mu y_\mu&=t_1,\\
V_1^2(y_1+y_2)+V_3^2y_3+\ldots+V_\mu^2y_\mu&=t_2,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\ldots\ldots\\
V_1^{\mu-1}(y_1+y_2)+V_2^{\mu-1}y_3+\ldots+V_\mu^{\mu-2}y_\mu&=t_{\mu-1}.
\end{aligned}$$

En opérant sur ces équations, comme nous l'avons fait sur les équations (5), on déterminera les inconnues

$$y_1+y_2,\ y_3,\ldots,\ y_\mu,$$

qui se trouveront exprimées respectivement en fonction rationnelle de

$$V_1 \text{ ou } V_2,\ V_3,\ldots,\ V_\mu.$$

Et généralement si l'équation

$$\psi(V) = 0$$

a α racines égales à V_1, 6 racines égales à V_2, etc., les équations (5), dont quelques-unes deviendront alors inutiles, ne pourront faire connaître que la somme des α valeurs de y, qui correspondent aux α valeurs de V égales à V_1, en fonction rationnelle de V_1 ; celle des 6 valeurs de y, qui correspondent aux 6 valeurs de V égales à V_2, en fonction rationnelle de V_2, et ainsi de suite. Voici comment on pourra, dans ce cas, déterminer les valeurs de y.

Supposons qu'on ait ces α valeurs de V égales entre elles,

$$V_1 = V_2 = . \quad . = V_\alpha;$$

on pourra calculer, en fonction de V_1, la somme

$$y_1 + y_2 + \ldots + y_\alpha.$$

On pourra aussi calculer, de la même manière, la somme des carrés de ces quantités, la somme de leurs cubes, etc., et enfin la somme de leurs puissances α; on pourra donc former (troisième leçon) l'équation de degré α, qui a pour racines les quantités $y_1, y_2, \ldots, y_\alpha$. Ainsi, quand l'équation en V a des racines égales, la détermination de la fonction y, semblable à V, peut dépendre d'une équation du second, ou du troisième, ou etc., degré.

On peut former, sans faire de nouveaux calculs, la somme des valeurs de y qui correspondent aux valeurs égales de V, et la déduire des équations (13). Supposons, par exemple, que $V_2 = V_1$, mais que les autres valeurs V_3, V_4, etc., soient différentes de V_1 ; augmentons les coefficients de l'équation proposée (1) de quantités infiniment petites, de manière que V_2 ne soit plus égal à V_1, et po-

sons $V_2 = V_1 + h$, h étant un infiniment petit : on aura

$$y_1 = \frac{\Theta(V_1)}{\psi'(V_1)}, \quad y_2 = \frac{\Theta(V_1 + h)}{\psi'(V_1 + h)}.$$

Soit

$$\psi(V) = (V - V_1)(V - V_1 - h)\psi_1(V);$$

on aura, en différentiant,

$$\psi'(V) = (V - V_1)(V - V_1 - h)\psi_1'(V) + [2(V - V_1) - h]\psi_1(V),$$

et, par suite,

$$\psi'(V_1) = -h\psi_1(V_1), \quad \psi'(V_1 + h) = h\psi_1(V_1 + h),$$

ou, en négligeant les puissances de h supérieures à la première dans $\psi'(V_1 + h)$,

$$\psi'(V_1 + h) = h\psi_1(V_1).$$

D'après cela, les valeurs de y_1 et y_2 seront

$$y_1 = \frac{-\Theta(V_1)}{h\psi_1(V_1)}, \quad y_2 = \frac{\Theta(V_1 + h)}{h\psi_1(V_1)};$$

donc

$$y_1 + y_2 = \frac{\Theta(V_1 + h) - \Theta(V_1)}{h\psi_1(V_1)}.$$

Cette équation est inexacte, puisque nous avons négligé les puissances de h supérieures à la première; mais elle sera exacte à la limite, pour $h = 0$, c'est-à-dire quand on égalera à zéro les quantités ajoutées aux coefficients de l'équation proposée. Or, pour $h = 0$, on a

$$\frac{\Theta(V_1 + h) - \Theta(V_1)}{h} = \Theta'(V_1)$$

et

$$\psi_1(V_1) = \lim \frac{\psi(V)}{(V - V_1)^2}, \quad \text{pour} \quad V = V_1,$$

c'est-à-dire

$$\psi_1(V_1) = \frac{\psi''(V_1)}{2};$$

on aura donc, enfin,

$$\frac{y_1 + y_2}{2} = \frac{\theta'(V)}{\psi''(V_1)},$$

et l'on ferait voir assez aisément que si l'on a, en général,

$$V_1 = V_2 = \ldots = V_\alpha,$$

on aura en même temps

$$(14) \qquad \frac{y_1 + y_2 + \ldots + y_\alpha}{\alpha} = \frac{\theta^{\alpha-1}(V_1)}{\psi^\alpha(V_1)};$$

en sorte qu'on obtiendra la moyenne arithmétique des valeurs de y qui correspondent aux valeurs de V égales à V_1, en prenant la valeur illusoire de y_1, donnée par les équations (13), et substituant au numérateur et au dénominateur de cette valeur de y_1, leurs dérivées d'ordre $\alpha - 1$ par rapport à V_1. La démonstration de l'équation (14) n'offre aucune difficulté; mais comme cette formule est seulement curieuse et ne nous sera d'aucune utilité, nous nous bornerons aux développements qui précèdent.

Méthode pour calculer une fonction des racines d'une équation, quand on connaît une autre fonction quelconque des racines.

La théorie qui vient d'être exposée peut être aisément étendue au cas où la fonction inconnue y n'est pas semblable à la fonction donnée V.

Nous désignerons toujours par $x_1, x_2, \ldots, x_m$ les m racines de l'équation proposée, et par M le produit $1.2.3\ldots m$. Si l'on applique simultanément aux deux

fonctions V et y les M substitutions que l'on peut faire, il en résultera pour V, M valeurs,

$$V_1,\ V_2,\ V_3,\ldots,\ V_M,$$

et pour y, M valeurs correspondantes

$$y_1,\ y_2,\ y_3,\ldots,\ y_M;$$

le nombre des valeurs distinctes de V ou de y, s'il n'est pas égal à M, sera un diviseur de M, ainsi que nous l'avons démontré au commencement de cette leçon. Il convient de distinguer deux cas :

1°. Supposons d'abord que les M valeurs de V soient distinctes, algébriquement parlant, ce qui n'empêchera pas que quelques-unes de ces valeurs ne puissent être numériquement égales, et ne faisons d'ailleurs aucune hypothèse sur le nombre des valeurs distinctes de y. Dans ce cas, la méthode précédemment exposée s'appliquera, sans modification, à la détermination de chaque valeur de y en fonction de la valeur correspondante de V. On aura toujours, en conservant nos mêmes notations,

$$y = \frac{T_0 V^{\mu-1} + T_1 V^{\mu-2} + \ldots + T_{\mu-2} V + T_{\mu-1}}{\mu V^{\mu-1} + (\mu-1) P_1 V^{\mu-2} + \ldots + 2 P_{\mu-2} V + P_{\mu-1}} = \frac{\theta(V)}{\psi'(V)};$$

seulement, on aura ici $\mu = M$, et en donnant à V successivement ses M valeurs, l'équation précédente fera connaître toutes les valeurs de y chacune répétées le même nombre de fois, et exprimées chacune par la valeur de V correspondante. Si l'équation $\psi(V) = 0$ a des racines égales, on opérera comme si V et y étaient des fonctions semblables.

2°. Supposons que le nombre des valeurs distinctes de V soit moindre que M : désignons-le par μ, et posons

$$M = n\mu;$$

les M valeurs de V

$$V_1, V_2, \ldots, V_M,$$

se partageront alors en μ groupes contenant chacun n valeurs égales. Soient

$$V_1, \; V_2, \ldots\ldots, V_n,$$
$$V_{n+1}, V_{n+2}, \ldots\ldots, V_{2n},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$V_{(\mu-1)n+1}, \ldots\ldots, V_{\mu n},$$

ces μ groupes, et désignons toujours par y_ρ la valeur de y correspondante à V_ρ.

Pour ramener ce cas à celui des fonctions semblables, désignons par z une fonction symétrique et rationnelle quelconque des quantités

$$y_1, y_2, \ldots, y_n,$$

il est évident que V et z seront des fonctions semblables; on pourra donc exprimer z en fonction rationnelle de V. Quand on aura ainsi calculé n fonctions symétriques des quantités $y_1, y_2, \ldots, y_n$, on pourra former l'équation du degré n, qui a pour racines ces n valeurs de y.

On voit, par ce qui précède, qu'on pourra toujours déterminer les racines x_1, $x_2, \ldots$, x_m d'une équation donnée, si l'on connait la valeur d'une fonction V de ces racines, pourvu que les $1.2.3\ldots m$ valeurs que prend cette fonction, quand on y permute les racines, soient différentes, non-seulement sous le rapport de la forme algébrique, mais encore au point de vue numérique.

En effet, on peut supposer que la fonction inconnue y se réduise à l'une quelconque des racines, à x_1 par exemple; alors on pourra exprimer x_1 en fonction rationnelle de V et des coefficients de l'équation proposée : si ensuite on suppose que y se réduise à une autre racine x_2, on pourra de même exprimer x_2 en fonction rationnelle

de V, et ainsi de suite. D'où il résulte que si la valeur donnée de V est commensurable, les racines de l'équation proposée seront toutes commensurables.

Mais si la fonction V n'a pas toutes ses valeurs distinctes, que l'on ait, par exemple,

$$V_1 = V_2 = V_3,$$

et si, faisant toujours $y = x_1$, les valeurs de y correspondantes sont

$$x_1,\ x_2,\ x_3,$$

la méthode précédente ne fera plus connaître ces racines, elle permettra seulement de former l'équation du troisième degré dont elles dépendent.

La théorie qui vient d'être exposée comprend tout ce que l'on sait de plus général sur l'abaissement des équations quand on connaît une relation entre les racines, car ce cas est évidemment le même que celui où l'on donne la valeur d'une fonction des racines.

DOUZIÈME LEÇON.

Application de la théorie exposée dans la leçon précédente. — Nouvelle démonstration d'un théorème établi dans cette leçon.

Application de la théorie exposée dans la leçon précédente.

Quoique la théorie exposée dans la précédente leçon soit très-simple, je ne crois pas inutile de montrer sur un exemple comment les calculs doivent être exécutés.

Nous nous proposerons de calculer l'une des trois racines x_1, x_2, x_3 de l'équation du troisième degré

$$x^3 - 6x^2 + 11x - 6 = 0,$$

x_1 par exemple, sachant que la fonction

$$V = x_1 + 2x_2 - 4x_3$$

est égale à 3.

Faisons

$$y = x_1,$$

et appliquons aux fonctions V et y les $1.2.3 = 6$ substitutions

$$\begin{pmatrix} x_1, x_2, x_3 \\ x_1, x_2, x_3 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_1, x_3, x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_2, x_3, x_1 \end{pmatrix},$$
$$\begin{pmatrix} x_1, x_2, x_3 \\ x_2, x_1, x_3 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_3, x_1, x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1, x_2, x_3 \\ x_3, x_2, x_1 \end{pmatrix};$$

il en résultera les six valeurs suivantes pour V et y :

$$\begin{aligned}
V_1 &= x_1 + 2x_2 - 4x_3, & y_1 &= x_1,\\
V_2 &= x_1 + 2x_3 - 4x_2, & y_2 &= x_1,\\
V_3 &= x_2 + 2x_3 - 4x_1, & y_3 &= x_2,\\
V_4 &= x_2 + 2x_1 - 4x_3, & y_4 &= x_2,\\
V_5 &= x_3 + 2x_1 - 4x_2, & y_5 &= x_3,\\
V_6 &= x_3 + 2x_2 - 4x_1, & y_6 &= x_3.
\end{aligned}$$

Soit

$$V^6 + P_1 V^5 + P_2 V^4 + P_3 V^3 + P_4 V^2 + P_5 V + P_6 = 0$$

l'équation qui a pour racines les six valeurs de V; on trouve

$$P_1 = 12, \quad P_2 = -2, \quad P_3 = -336,$$
$$P_4 = -287, \quad P_5 = 2052, \quad P_6 = 2016;$$

il faut calculer ensuite les quantités $t_0, t_1, t_2, t_3, t_4, t_5$, telles que

$$\sum y \quad = t_0,$$
$$\sum V y = t_1,$$
$$\sum V^2 y = t_2,$$
$$\sum V^3 y = t_3,$$
$$\sum V^4 y = t_4,$$
$$\sum V^5 y = t_5,$$

par la méthode des fonctions symétriques : on trouve ainsi

$$t_0 = 12, \quad t_1 = -16, \quad t_2 = 264,$$
$$t_3 = -1240, \quad t_4 = 11592, \quad t_5 = -80296;$$

et en posant, comme précédemment,

$$T_5 = t_5 + P_1 t_4 + P_2 t_3 + P_3 t_2 + P_4 t_1 + P_5 t_0,$$
$$T_4 = t_4 + P_1 t_3 + P_2 t_2 + P_3 t_1 + P_4 t_0,$$
$$T_3 = t_3 + P_1 t_2 + P_2 t_1 + P_3 t_0,$$
$$T_2 = t_2 + P_1 t_1 + P_2 t_0,$$
$$T_1 = t_1 + P_1 t_0,$$
$$T_0 = t_0,$$

on a

$$T_5 = 1800,\quad T_4 = -1884,\quad T_3 = -2072,$$
$$T_2 = 48,\quad T_1 = 128,\quad T_0 = 12.$$

Maintenant la formule générale

$$y = \frac{T_0 V^5 + T_1 V^4 + T_2 V^3 + T_3 V^2 + T_4 V + T_5}{6 V^5 + 5 P_1 V^4 + 4 P_2 V^3 + 3 P_3 V^2 + 2 P_4 V + P_5},$$

où l'on doit affecter y et V de mêmes indices, devient

$$y = \frac{12 V^5 + 128 V^4 + 48 V^3 - 2072 V^2 - 1884 V + 1800}{6 V^5 + 60 V^4 - 8 V^3 - 1008 V^2 - 574 V + 2052}.$$

Pour avoir la racine x_1, il faut faire $V = 3$, et l'on trouve ainsi

$$x_1 = \frac{-7920}{-2640} = 3.$$

On voit, par ce qui précède, que les calculs auxquels conduit notre théorie sont d'une longueur rebutante, même dans les cas les plus simples; mais il ne faut pas oublier que nous nous plaçons au point de vue théorique, bien plutôt qu'à celui de l'application. Toutefois ces calculs se simplifient en suivant une nouvelle marche indiquée par Gallois et que nous allons faire connaître.

Nouvelle démonstration d'un théorème établi dans la leçon précédente.

THÉORÈME. — *Si*

(1) $$f(x) = 0$$

est une équation quelconque de degré m, *mais qui n'a pas de racines égales, et que*

$$V = \varphi(x_1, x_2, \ldots, x_m)$$

soit une fonction rationnelle des racines $x_1, x_2, \ldots, x_m$

de l'équation (1), *tellement choisie, que les* 1.2.3...m *valeurs qu'elle prend, quand on y permute les racines, soient toutes différentes, on pourra exprimer les* m *racines* $x_1, x_2, \ldots, x_m$ *en fonction rationnelle de* V.

Voici comment Gallois démontre ce théorème dans le Mémoire inséré au tome XI du *Journal de Mathématiques* de M. Liouville.

Nous désignerons par V_1 la valeur donnée de V, et par

$$V_1, V_2, \ldots, V_\mu$$

les $\mu = 1.2.3\ldots(m-1)$ valeurs que prend V, quand on y permute les $m-1$ racines

$$x_2, x_3, \ldots, x_m,$$

sans changer la place de x_1. On aura alors une équation en V du degré μ, savoir :

$$(2) \qquad (V - V_1)(V - V_2)\ldots(V - V_\mu) = 0,$$

dont les racines V_1, V_2, etc., seront toutes différentes et dont les coefficients, qui sont des fonctions symétriques des racines $x_2, x_3, \ldots, x_m$ de l'équation

$$\frac{f(x)}{x - x_1} = 0,$$

s'exprimeront rationnellement par les coefficients de cette équation, c'est-à-dire en fonction de x_1 et des coefficients de l'équation proposée (1). Par suite, l'équation (2) pourra être mise sous la forme

$$(3) \qquad F(V, x_1) = 0,$$

F désignant une fonction rationnelle de V et de x_1. Or l'équation (2), ou l'équation (3), est satisfaite pour $V = V_1$; on aura donc identiquement

$$F(V_1, x_1) = 0.$$

D'où il suit que l'équation

$$(4)\qquad F(V_1, x) = 0$$

sera satisfaite pour

$$x = x_1,$$

et, par conséquent, les équations (1) et (4) auront une racine commune x_1. Je dis, de plus, que ces équations ne sauraient avoir d'autre racine commune. Supposons, en effet, que l'équation (4) soit satisfaite pour $x = x_2$, on aura identiquement

$$F(V_1, x_2) = 0;$$

par suite, l'équation

$$(5)\qquad F(V, x_2) = 0$$

sera satisfaite pour $V = V_1$. Or l'équation (5) se déduit de l'équation (3), ou de l'équation (2), en changeant x_1 et x_2 l'une dans l'autre : d'ailleurs, par ce changement, les quantités $V_1, V_2, \ldots, V_\mu$ se changent en d'autres V'_1, $V'_2, \ldots, V'_\mu$, toutes distinctes des premières par hypothèse; l'équation (5) peut donc se mettre sous la forme

$$(V - V'_1)(V - V'_2)\ldots(V - V'_\mu) = 0,$$

et l'on voit qu'elle ne saurait avoir V_1 pour racine.

Les équations (1) et (4) n'ayant que la seule racine commune x_1, on déterminera aisément cette racine. Pour cela on cherchera le plus grand commun diviseur entre $f(x)$ et $F(V_1, x)$, et l'on poussera l'opération jusqu'à ce qu'on obtienne un reste du premier degré en x : en égalant à zéro ce reste, on aura une équation qui fera connaître la valeur de x_1,

$$x_1 = \psi(V_1) \quad \text{ou} \quad x_1 = \psi(V);$$

et cette valeur de x_1 sera évidemment rationnelle en V,

car l'opération du plus grand commun diviseur ne peut jamais introduire de radicaux.

On pourrait opérer de même pour trouver les autres racines, et l'on aurait ainsi pour toutes ces racines des expressions rationnelles, telles que

$$x_1 = \psi_1(V), \quad x_2 = \psi_2(V), \ldots, \quad x_m = \psi_m(V).$$

COROLLAIRE I. — L'équation en V du degré $M = 1.2.3\ldots m$, qui a pour racines toutes les M valeurs de V, et dont les coefficients s'expriment rationnellement par ceux de l'équation proposée, jouit d'une propriété remarquable qui consiste en ce que toutes ses racines peuvent être exprimées rationnellement par l'une quelconque d'entre elles. Soient, en effet, V et V_1 deux des valeurs de V; V_1 est une fonction rationnelle des racines $x_1, x_2, \ldots, x_m$, lesquelles, d'après ce qui précède, sont des fonctions rationnelles de V : on aura donc

$$V_1 = \Theta(V),$$

Θ désignant une fonction rationnelle.

COROLLAIRE II. — On peut aussi déduire, de ce qui précède, la proposition suivante :

Étant données tant d'irrationnelles algébriques qu'on voudra, on peut toujours les exprimer toutes en fonction rationnelle d'une même irrationnelle.

Soient, en effet,

$$x_1, \ x_2, \ldots, \ x_n,$$

n irrationnelles algébriques quelconques; on pourra former une équation d'un certain degré m, à coefficients commensurables, dont ces n quantités seront racines, et qui n'aura pas de racines égales. Soient

$$x_1, \ x_2, \ldots, \ x_m$$

les m racines de cette équation, et désignons par V une

fonction rationnelle de ces m racines telle, que les valeurs qu'elle prend par les substitutions soient toutes distinctes. V sera une irrationnelle algébrique en fonction de laquelle les n irrationnelles données pourront s'exprimer rationnellement, d'après le théorème précédent.

Nous admettons comme évident qu'on peut toujours former une fonction rationnelle de m quantités inégales telle, que les $1.2.3\ldots m$ valeurs qu'on en déduit par les substitutions soient différentes.

Application à un exemple. — Le théorème précédent fournit une méthode beaucoup plus simple que celle qui résulte de la théorie de Lagrange, pour déterminer les racines d'une équation quand on se donne une fonction de ces racines. Nous prendrons comme exemple le cas de l'équation du troisième degré.

Soit l'équation

$$(1) \qquad x^3 + p_1 x^2 + p_2 x + p_3 = 0,$$

et posons

$$V = ax_1 + bx_2 + cx_3.$$

En permutant les lettres x_2 et x_3, on aura ces deux valeurs de V,

$$V_1 = ax_1 + bx_2 + cx_3,$$
$$V_2 = ax_1 + bx_3 + cx_2;$$

l'équation en V sera alors

$$(V - V_1)(V - V_2) = 0,$$

ou

$$V^2 - [2ax_1 + (b + c)(x_2 + x_3)]V$$
$$+ [a^2x_1^2 + a(b+c)x_1(x_2+x_3) + bc(x_2^2+x_3^2) + (b^2+c^2)x_2x_3] = 0.$$

On peut chasser x_2 et x_3 de cette équation à l'aide des relations

$$x_2 + x_3 = -p_1 - x_1,$$
$$x_2x_3 = p_2 - x_1(x_2 + x_3) = p_2 + p_1x_1 + x_1^2,$$
$$x_2^2 + x_3^2 = (p_1^2 - 2p_2) - x_1^2,$$

et l'on aura

$$(2)\left\{\begin{array}{c} V^2 - [(2a - b - c)x_1 - p_1(b + c)]V \\ + \left[\begin{array}{c} (a^2 + b^2 + c^2 - ab - ac - bc)x_1^2 \\ + (b^2 + c^2 - ab - ac)p_1 x_1 + bc p_1^2 - (b - c)^2 p_2 \end{array}\right] \end{array}\right\} = 0.$$

Il faudra maintenant, pour avoir x_1, faire $x = x_1$ dans le premier membre de l'équation (1) et chercher le plus grand commun diviseur entre le polynôme que l'on obtiendra ainsi et le premier membre de l'équation (2) : il n'y a même aucun calcul à faire dans le cas particulier où l'on a

$$a^2 + b^2 + c^2 - ab - ac - bc = 0;$$

car alors l'équation (2) ne contient plus que la première puissance de x_1, et elle en fait connaître immédiatement la valeur. Ce cas simple se présente si l'on prend pour a, b, c les trois racines cubiques de l'unité.

Soit α une racine cubique imaginaire de l'unité, et posons

$$a = 1, \quad b = \alpha, \quad c = \alpha^2,$$

on aura, en remarquant que $\alpha + \alpha^2 + 1 = 0$,

$$x_1 = \frac{V^2 - p_1 V + (p_1^2 - 3p_2)}{3V}.$$

TREIZIÈME LEÇON.

Propriétés des racines de l'équation binôme. Des racines primitives et de leur nombre. — Digression sur la résolution numérique de l'équation à laquelle se ramène l'équation binôme, quand on lui applique la méthode d'abaissement des équations réciproques. Exposition de la méthode de M. Sturm pour la séparation des racines.

Les racines de l'unité jouent un rôle important dans la théorie de la résolution algébrique des équations, dont nous allons bientôt nous occuper; je crois donc utile de rappeler ici les propriétés de ces racines, dont quelques-unes sont démontrées dans les Traités élémentaires d'Algèbre.

Propriétés des racines de l'équation binôme. Des racines primitives et de leur nombre.

I. ***Les racines communes à deux équations binômes, telles que***

$$x^m = 1, \quad x^n = 1,$$

sont également racines de l'équation

$$x^\theta = 1,$$

où θ désigne le plus grand commun diviseur des nombres m et n.

Supposons, en effet, que l'on ait à la fois

$$x^m = 1 \quad \text{et} \quad x^n = 1;$$

soit $m > n$, et désignons par q le quotient et par r le reste de la division de m par n, en sorte que $m = nq + r$:

on aura

$$\alpha^{nq+r} = 1, \quad \text{ou} \quad \alpha^{nq}.\alpha^r = 1.$$

Mais, à cause de $\alpha^n = 1$, on a aussi $\alpha^{nq} = 1$; donc

$$\alpha^r = 1.$$

D'où l'on conclut aisément que si $r, r', r'', \ldots, \theta$ sont les restes auxquels conduit la recherche du plus grand commun diviseur des entiers m et n, on aura

$$\alpha^r = 1, \ \alpha^{r'} = 1, \ldots, \ \alpha^\theta = 1,$$

et, par conséquent, toute racine commune, α, aux deux équations proposées, est aussi racine de

$$x^\theta = 1.$$

Il est évident d'ailleurs que, réciproquement, les racines de cette dernière équation appartiennent aux deux équations proposées.

Il résulte de là que si m et n sont premiers entre eux, les deux équations

$$x^m = 1, \ x^n = 1$$

n'ont d'autre racine commune que l'unité, et que, si m est un nombre premier, l'équation

$$x^m = 1$$

n'a de racine commune autre que l'unité, avec aucune équation de même forme et de degré moindre.

II. *Si α désigne une racine quelconque de l'équation binôme*

$$x^m = 1,$$

toute puissance de α est aussi racine de la même équation.

L'équation

$$\alpha^m = 1$$

entraîne, en effet,

$$\alpha^{mk} = 1, \quad \text{ou} \quad (\alpha^k)^m = 1,$$

et, par conséquent, tous les termes de la série

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots$$

sont racines de l'équation proposée. Or, à cause de $\alpha^m = 1$, on a aussi

$$\alpha^{m+1} = \alpha,\quad \alpha^{m+2} = \alpha^2,\ldots;$$

d'où il suit que la série précédente contient au plus, comme cela doit être, m quantités distinctes, savoir :

$$\alpha,\ \alpha^2,\ \alpha^3,\ \ldots,\ \alpha^{m-1},\ \alpha^m \text{ ou } 1.$$

Si m est un nombre *premier*, et si α n'est pas égal à l'unité, les m termes de la série précédente sont différents; car si l'on avait, par exemple,

$$\alpha^{n+n'} = \alpha^{n'},$$

n' et $n + n'$ étant inférieurs à m, on aurait, en divisant par $\alpha^{n'}$,

$$\alpha^n = 1;$$

ce qui ne peut être, puisque l'équation $x^m = 1$ ne saurait avoir d'autre racine commune que l'unité avec $x^n = 1$. Il en résulte ce théorème :

Si m est un nombre premier, et que α soit une racine quelconque de l'équation

$$x^m = 1,$$

autre que l'unité, les m racines de cette équation seront représentées par

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{m-1},\ \alpha^m.$$

Cette proposition n'a plus lieu lorsque m est un nombre composé, et qu'on prend pour α une racine quelconque de

$$x^m = 1;$$

mais elle aura lieu évidemment, d'après ce qui précède, si l'on prend pour α une racine qui n'appartienne en

même temps à aucune équation $x^n = 1$ de degré n inférieur à m.

Cela posé, nous appellerons *racines primitives* de l'équation binôme

$$x^m = 1,$$

les racines de cette équation qui n'appartiennent à aucune équation de degré moindre et de même forme, telle que

$$x^n = 1.$$

Si m est premier, toute racine de $x^m = 1$, autre que 1, est une racine primitive; et, dans tous les cas, chaque racine primitive jouit de la propriété de pouvoir donner toutes les racines par ses diverses puissances.

Nous allons démontrer actuellement l'existence des racines primitives pour toute équation binôme, de degré non premier, et déterminer en même temps le nombre de ces racines primitives.

III. Considérons d'abord le cas où le degré de l'équation binôme

$$x^m = 1$$

est une puissance d'un nombre premier p, et soit

$$m = p^\mu;$$

toute racine non primitive de l'équation

$$x^{p^\mu} = 1$$

doit appartenir à une équation telle que

$$x^\theta = 1,$$

où θ désigne un diviseur de p^μ : mais tout diviseur de p^μ, autre que p^μ lui-même, doit diviser $p^{\mu-1}$; donc les racines de l'équation précédente, et, par suite, toutes les racines *non primitives* de la proposée, doivent appartenir

à l'équation

$$x^{p^{\mu-1}} = 1.$$

D'ailleurs toutes les racines de cette dernière appartiennent évidemment à la proposée; le nombre des racines non primitives de la proposée est donc $p^{\mu-1}$, et, par conséquent, celui des racines primitives est

$$p^{\mu} - p^{\mu-1}, \quad \text{ou} \quad p^{\mu}\left(1 - \frac{1}{p}\right), \quad \text{ou} \quad m\left(1 - \frac{1}{p}\right).$$

Nous allons faire connaître la manière dont sont formées les racines primitives.

Considérons toujours l'équation

$$(1) \qquad x^{p^{\mu}} = 1,$$

et soient θ_1 une racine quelconque de l'équation

$$x^p = 1,$$

θ_2 une racine quelconque de

$$x^p = \theta_1,$$

θ_3 une racine quelconque de

$$x^p = \theta_2,$$

et ainsi de suite, jusqu'à ce qu'on obtienne une dernière équation

$$x^p = \theta_{\mu-1},$$

dont nous désignerons par θ_μ une racine quelconque. Si l'on fait

$$(2) \qquad \alpha = \theta_1\theta_2 \ldots \theta_{\mu-1}\theta_\mu,$$

cette expression de α, qui a p^{μ} valeurs, puisque θ_1 a p valeurs, qu'à chacune d'elles correspondent p valeurs de θ_2, etc., donnera précisément les p^{μ} racines de l'équation (1).

On voit d'abord que les valeurs de α satisfont à l'équation (1), car on a

$$6_1^{p} = 1,\quad 6_2^{p^2} = 1,\quad 6_3^{p^3} = 1, \ldots,\quad 6_{\mu-1}^{p^{\mu-1}} = 1,\quad 6_\mu^{p^\mu} = 1,$$

et, par suite,

$$\alpha^{p^\mu} = 1.$$

Il suffit donc de démontrer que les p^μ valeurs de α sont distinctes. Supposons que deux de ces valeurs soient égales entre elles, que l'on ait, par exemple,

$$(3) \qquad 6_1 6_2 6_3 \ldots 6_{\mu-1} 6_\mu = 6'_1\, 6'_2\, 6'_3 \ldots 6'_{\mu-1}\, 6'_\mu;$$

en élevant cette égalité à la puissance p, et se rappelant que

$$(4) \qquad \begin{cases} 6_1^p = 1, & 6_2^p = 6_1, \ldots, & 6_\mu^p = 6_{\mu-1}, \\ 6_1'^p = 1, & 6_2'^p = 6'_1, \ldots, & 6_\mu'^p = 6'_{\mu-1}, \end{cases}$$

on aura

$$(5) \qquad 6_1 6_2 6_3 \ldots 6_{\mu-1} = 6'_1\, 6'_2\, 6'_3 \ldots 6'_{\mu-1}.$$

Des égalités (3) et (5) on tire

$$6_\mu = 6'_\mu;$$

en opérant sur l'égalité (5) comme nous venons de faire sur l'égalité (3), on obtiendra

$$6_{\mu-1} = 6'_{\mu-1},$$

et, en continuant ainsi, on arrivera à cette conséquence : que l'égalité (3) ne peut exister à moins que les quantités $6_1, 6_2, \ldots, 6_\mu$ ne soient respectivement égales aux quantités $6'_1, 6'_2, \ldots, 6'_\mu$. D'où il suit que l'équation (2) donnera effectivement toutes les racines de l'équation (1).

Cherchons maintenant quelles sont celles de ces racines qui sont primitives. Comme nous l'avons déjà remarqué, les racines non primitives de l'équation (1) sont celles qui satisfont à l'équation

$$x^{p^{\mu-1}} = 1.$$

Supposons donc que l'on ait

$$(6_1 6_2 6_3 \ldots 6_{\mu-1} 6_\mu)^{p^{\mu-1}} = 1;$$

en supprimant les facteurs égaux à l'unité, cette équation se réduit à

$$(6) \qquad 6_\mu^{p^{\mu-1}} = 1.$$

Mais des égalités (4) on déduit

$$6_\mu^{p^{\mu-1}} = 6_{\mu-1}^{p^{\mu-2}} = 6_{\mu-2}^{p^{\mu-3}} = \ldots = 6_2^p = 6_1;$$

par suite, l'équation (6) exige que

$$6_1 = 1.$$

Par où l'on voit que la valeur de α donnée par la formule (2) sera une racine primitive ou non primitive de l'équation (1), suivant que 6_1 sera différent de 1 ou égal à 1.

De ce qui précède on peut conclure la proposition suivante :

Théorème. — *La résolution de l'équation binôme $x^m = 1$, dont le degré m est une puissance μ d'un nombre premier p, se ramène à déterminer une racine 6_1 autre que l'unité de l'équation $x^p = 1$, une racine 6_2 quelconque de l'équation $x^p = 6_1$, puis une racine quelconque 6_3 de $x^p = 6_2$, etc.*

Car on aura, par ce moyen, une racine primitive de l'équation proposée, laquelle donnera toutes les autres par ses diverses puissances.

IV. Considérons maintenant le cas général où le degré m de l'équation binôme

(1) $$x^m = 1$$

est un nombre composé quelconque; décomposons ce nombre en ses facteurs premiers, et soit

$$m = p^\mu q^\nu \ldots r^\lambda,$$

$p, q, \ldots, r$ désignant des nombres premiers quelconques inégaux.

Écrivons les équations

(2) $$x^{p^\mu} = 1, \quad x^{q^\nu} = 1, \ldots, \quad x^{r^\lambda} = 1;$$

désignons par β une racine quelconque de la première, par γ une racine quelconque de la seconde, etc., par δ une racine quelconque de la dernière, et posons

(3) $$\alpha = \beta\gamma\ldots\delta.$$

Cette expression de α a m valeurs, puisque $\beta, \gamma, \ldots, \delta$ ont respectivement $p^\mu, q^\nu, \ldots, r^\lambda$ valeurs; je dis que ce sont précisément les m racines de l'équation (1).

Il est d'abord évident que la précédente valeur de α satisfait à l'équation (1), car on a

$$\beta^{p^\mu} = 1, \quad \gamma^{q^\nu} = 1, \ldots, \quad \delta^{r^\lambda} = 1,$$

et, par suite,

$$\beta^m = 1, \quad \gamma^m = 1, \ldots, \quad \delta^m = 1;$$

d'où

$$\alpha^m = 1.$$

Il faut prouver maintenant que les m valeurs de α sont différentes. Supposons, en effet, que deux de ces valeurs de α soient égales, que l'on ait, par exemple,

$$\beta'\gamma'\ldots\delta' = \beta''\gamma''\ldots\delta'';$$

comme les quantités $\beta', \gamma', \ldots, \delta'$ ne sont pas toutes égales respectivement à $\beta'', \gamma'', \ldots, \delta''$, admettons que β' diffère

de $6''$, et élevons l'égalité précédente à la puissance $q^{\nu}\ldots r^{\lambda}$, on aura

$$(6'\gamma'\ldots\delta')^{q^{\nu}\ldots r^{\lambda}}=(6''\gamma''\ldots\delta'')^{q^{\nu}\ldots r^{\lambda}},$$

et, en supprimant les facteurs égaux à 1,

$$6'^{q^{\nu}\ldots r^{\lambda}}=6''^{q^{\nu}\ldots r^{\lambda}};$$

mais $6'$ et $6''$ étant deux racines distinctes de l'équation $x^{p^{\mu}}=1$, peuvent s'exprimer par deux puissances d'une même racine primitive 6 de cette équation; posons donc

$$6'=6^{n+n'},\quad 6''=6^{n'},$$

n' et n étant $<p^{\mu}$. Alors la dernière égalité deviendra

$$6^{(n+n')q^{\nu}\ldots r^{\lambda}}=6^{n'q^{\nu}\ldots r^{\lambda}},$$

ou, simplement,

$$6^{nq^{\nu}\ldots r^{\lambda}}=1;$$

d'où il suit que 6 est une racine commune aux deux équations

$$x^{p^{\mu}}=1,\quad x^{nq^{\nu}\ldots r^{\lambda}}=1,$$

et satisfait, par conséquent, à l'équation

$$x^{\theta}=1,$$

θ désignant le plus grand commun diviseur à p^{μ} et $nq^{\nu}\ldots r^{\lambda}$. Mais ce plus grand commun diviseur θ est, au plus, égal à n, et, par conséquent, il est inférieur à p^{μ}; donc 6 n'est pas, comme nous l'avons supposé, une racine primitive de $x^{p^{\mu}}=1$.

On voit, par là, que la formule (3) donnera bien les m racines de l'équation (1).

Cela posé, je dis que si $6, \gamma, \ldots, \delta$ désignent des

racines primitives de celles des équations (2) auxquelles elles appartiennent respectivement, la valeur de α donnée par la formule (3) sera une racine primitive de l'équation (1).

Si, en effet, le contraire a lieu, α satisfera à une équation

$$x^{\theta} = 1,$$

dont le degré θ est un diviseur de m, et il y aura au moins un facteur premier, parmi ceux de m, qui entrera dans θ un moins grand nombre de fois que dans m : supposons que le facteur premier p soit dans ce cas, θ divisera $p^{\mu-1} q^{\nu} \ldots r^{\lambda}$, et, par suite, α sera racine de l'équation

$$(4) \qquad x^{p^{\mu-1} q^{\nu} \ldots r^{\lambda}} = 1;$$

on aura donc

$$(6\gamma \ldots \delta)^{p^{\mu-1} q^{\nu} \ldots r^{\lambda}} = 1.$$

Mais

$$\gamma^{q^{\nu}} = 1, \ldots, \quad \delta^{r^{\lambda}} = 1,$$

donc

$$6^{p^{\mu-1} q^{\nu} \ldots r^{\lambda}} = 1;$$

d'où il suit que 6 est racine de l'équation (4); or elle l'est aussi de la première des équations (2), d'ailleurs, le plus grand commun diviseur entre les degrés de ces deux équations est $p^{\mu-1}$; donc 6 est racine de l'équation

$$x^{p^{\mu-1}} = 1;$$

mais cela est contre l'hypothèse, puisque 6 représente une racine primitive de la première des équations (2).

Il résulte, de là, que si l'on ne prend pour $6, \gamma, \ldots, \delta$, que des racines primitives, de la première, de la seconde, etc., de la dernière des équations (2), la formule (3) ne donnera que des racines primitives pour

l'équation (1). Il est d'ailleurs facile de voir que si $\mathfrak{b}$, ou $\gamma, \ldots$, ou δ n'est pas une racine primitive de celle des équations (2), à laquelle elle appartient, la valeur de α donnée par la formule (3) ne sera pas non plus une racine primitive de l'équation (1). Supposons, en effet, que $\mathfrak{b}$ ne soit pas une racine primitive de $x^{p^\mu} = 1$; on aura alors

$$\mathfrak{b}^{p^{\mu-1}} = 1, \quad \gamma^{q^\nu} = 1, \ldots, \quad \delta^{r^\lambda} = 1,$$

et, par suite,

$$(\mathfrak{b}\gamma\ldots\delta)^{p^{\mu-1}q^\nu\ldots r^\lambda} = 1;$$

ce qui montre que α ou $\mathfrak{b}\gamma\ldots\delta$ satisfait à une équation binôme de degré inférieur à m.

On peut maintenant connaître le nombre des racines primitives de l'équation (1). En effet, le nombre des racines primitives $\mathfrak{b}$ est, comme on l'a vu précédemment, $p^\mu\left(1-\frac{1}{p}\right)$, celui des racines primitives γ est de même $q^\nu\left(1-\frac{1}{q}\right)$, etc.; donc le nombre des racines primitives α de l'équation (1) est

$$p^\mu q^\nu \ldots r^\lambda \left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\cdots\left(1-\frac{1}{r}\right),$$

ou

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\cdots\left(1-\frac{1}{r}\right).$$

On peut aussi énoncer la proposition suivante :

Théorème. — *La résolution de l'équation binôme $x^m = 1$, où m est un nombre composé quelconque, se ramène à la résolution des équations de même forme, et qui ont respectivement pour degrés les nombres premiers ou puissances de nombres premiers qui divisent le nombre m.*

V. Soient $\alpha, \mathfrak{b}, \gamma, \ldots, \omega$ les m racines de l'équation

$x^m = 1$, ou

$$x^m - 1 = 0,$$

m étant quelconque. On aura, par les formules de Newton (première leçon), les relations suivantes :

$$\alpha + 6 + \gamma + \ldots\ldots\ldots\ldots + \omega = 0,$$
$$\alpha^2 + 6^2 + \gamma^2 + \ldots\ldots\ldots\ldots + \omega^2 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha^{m-1} + 6^{m-1} + \gamma^{m-1} + \ldots + \omega^{m-1} = 0,$$
$$\alpha^m + 6^m + \gamma^m + \ldots\ldots\ldots\ldots + \omega^m = m;$$

et, généralement, à cause de $\alpha^{m+k} = \alpha^k$, la somme

$$\alpha^\mu + 6^\mu + \gamma^\mu + \ldots + \omega^\mu$$

sera égale à m ou à o, suivant que μ sera divisible ou non divisible par m.

VI. Quant à l'équation binôme plus générale

$$y^m = a,$$

elle se ramène à la forme

$$x^m = 1,$$

si l'on pose

$$y = x\sqrt[m]{a},$$

$\sqrt[m]{a}$ désignaut l'une quelconque des quantités qui ont a pour puissance $m^{ième}$.

On peut démontrer, à l'égard de ces extractions de racines $m^{ièmes}$, un théorème tout semblable à celui qui concerne les racines $m^{ièmes}$ de l'unité, lorsque m est un nombre composé.

Supposons d'abord que m soit le produit de deux nombres premiers entre eux p et q, on aura

$$\sqrt[m]{a} = a^{\frac{1}{pq}};$$

or on peut toujours trouver deux entiers ξ et υ tels, que l'on ait

$$p\xi + q\upsilon = 1,$$

puisque p et q sont premiers entre eux : on aura donc

$$\sqrt[m]{a} = a^{\frac{p\xi + q\upsilon}{pq}} = a^{\frac{\xi}{q}} . a^{\frac{\upsilon}{p}} = \sqrt[q]{a^\xi} . \sqrt[p]{a^\upsilon}.$$

Ainsi l'extraction d'une racine de degré pq se ramène toujours, lorsque p et q sont premiers entre eux, à l'extraction de deux racines, l'une du degré p, l'autre du degré q.

On a, par exemple, quel que soit a,

$$\sqrt[6]{a} = \sqrt{a} . \sqrt[3]{\frac{1}{a}}.$$

Et, en général, si

$$m = p.q\ldots r,$$

$p, q, \ldots, r$ désignant des nombres quelconques premiers entre eux, deux à deux, on pourra écrire

$$\sqrt[m]{a} = \sqrt[p]{a^\xi} . \sqrt[q]{a^\upsilon} \ldots \sqrt[r]{a^\omega},$$

formule dans laquelle $\xi, \upsilon, \ldots, \omega$ sont des nombres entiers positifs ou négatifs.

Digression sur la résolution numérique de l'équation à laquelle se ramène l'équation binôme, quand on lui applique la méthode d'abaissement des équations réciproques. Exposition de la méthode de M. Sturm, pour la séparation des racines.

J'exposerai ici, à l'occasion des équations binômes qui viennent de nous occuper, la belle méthode de M. Sturm, pour démontrer la réalité des racines de certaines classes

d'équations et effectuer ensuite la séparation de ces racines.

Considérons l'équation binôme

$$(1) \qquad x^m - 1 = 0,$$

où m est un nombre impair quelconque $2\mu + 1$. En divisant l'équation (1) par $x - 1$, elle devient

$$(2) \qquad x^{2\mu} + x^{2\mu-1} + \ldots + x^2 + x + 1 = 0;$$

et l'on transforme, comme on sait, cette équation (2), conformément à la méthode des équations réciproques, en une autre du degré μ, en la divisant par x^μ, et posant ensuite

$$x + \frac{1}{x} = z;$$

l'équation (2), divisée par x^μ, devient

$$\left(x^\mu + \frac{1}{x^\mu}\right) + \left(x^{\mu-1} + \frac{1}{x^{\mu-1}}\right) + \ldots + \left(x + \frac{1}{x}\right) + 1 = 0,$$

ou

$$(3) \qquad V_\mu + V_{\mu-1} + \ldots + V_2 + V_1 + 1 = 0,$$

en faisant généralement

$$V_n = x^n + \frac{1}{x^n};$$

on peut exprimer facilement $V_2, V_3, \ldots, V_\mu$, en fonction de z, de la manière suivante :

Si l'on multiplie les deux équations

$$V_{n-1} = x^{n-1} + \frac{1}{x^{n-1}},$$

$$z = x + \frac{1}{x},$$

on a

$$z V_{n-1} = \left(x^n + \frac{1}{x^n}\right) + \left(x^{n-2} + \frac{1}{x^{n-2}}\right) = V_n + V_{n-2},$$

d'où

(4) $$V_n = z V_{n-1} - V_{n-2}.$$

Cette relation fait connaître la valeur de chaque fonction V_n en z, quand on connaît les deux précédentes. Or les deux premières V_0 et V_1 sont connues : on a

$$V_1 = x + \frac{1}{x} = z, \quad V_0 = x^0 + \frac{1}{x^0} = 2;$$

on pourra donc, à l'aide de l'équation (4), calculer les valeurs des fonctions V_2, V_3, etc.

On trouve ainsi

(5) $$\left\{\begin{array}{l} V_0 = 2, \\ V_1 = z, \\ V_2 = z^2 - 2, \\ V_3 = z^3 - 3z, \\ V_4 = z^4 - 4z^2 + 2, \\ V_5 = z^5 - 5z^3 + 5z, \\ V_6 = z^6 - 6z^4 + 9z^2 - 2, \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

Il serait assez difficile de déduire de ces formules l'expression générale de V_n. Nous donnerons, dans la prochaine leçon, le moyen de former cette expression, et nous nous bornerons pour le moment aux remarques suivantes :

1°. V_n est un polynôme du degré n en z, qui ne renferme que des puissances de z de même parité que n;

2°. Les deux premiers termes de V_n sont $z^n - nz^{n-2}$.

En effet, l'équation (4) fait voir que si V_{n-1} et V_{n-2} satisfont à ces conditions, V_n y satisfera également, et l'on voit, à l'inspection des équations (5), que V_2, V_3, V_4, V_5 et V_6 y satisfont; d'où l'on conclut immédiatement la démonstration.

Posons maintenant

$$(6) \qquad U_n = V_n + V_{n-1} + \ldots + V_2 + V_1 + 1;$$

U_n sera un polynôme du degré n en z, et l'équation (3), à laquelle nous avons ramené l'équation (1), sera

$$U_\mu = 0.$$

Les fonctions U_n sont susceptibles d'un mode de formation identique à celui des fonctions V_n, c'est-à-dire que l'on a

$$U_n = z\,U_{n-1} - U_{n-2}.$$

En effet, on a, par l'équation (4),

$$V_n = z\,V_{n-1} - V_{n-2},$$
$$V_{n-1} = z\,V_{n-2} - V_{n-3},$$
$$\ldots\ \ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ \ldots\ldots\ldots\ldots$$
$$V_2 = z\,V_1 - 2;$$

en ajoutant ces équations, et ayant égard à l'équation (6), il vient

$$U_n - V_1 - 1 = z\,(U_{n-1} - 1) - (U_{n-2} + 1);$$

et comme $V_1 = z$,

$$(7) \qquad U_n = z\,U_{n-1} - U_{n-2},$$

équation qui se déduit de (4), en remplaçant la lettre V par U.

Comme on a

$$U_0 = 1, \quad U_1 = V_1 + 1 = z + 1,$$

l'équation (7) donnera successivement les valeurs des fonctions U_2, U_3, etc.; on trouve ainsi

$$U_0 = 1;$$
$$U_1 = z + 1,$$
$$U_2 = z^2 + z - 1,$$
$$U_3 = z^3 + z^2 - 2z - 1,$$
$$\dots\dots\dots\dots$$

Quant à l'expression générale de U_n, elle se déduit très-aisément de celle de V_n, ainsi que nous le verrons dans la prochaine leçon.

Nous allons à présent démontrer la réalité des racines des équations

$$V_\mu = 0, \quad U_\mu = 0,$$

et indiquer en même temps le moyen de séparer ces racines.

De l'équation $V_\mu = 0$. — Nous nous occuperons d'abord de l'équation

$$(1) \qquad V_\mu = 0.$$

Considérons, avec M. Sturm, la suite des fonctions

$$V_\mu,\ V_{\mu-1},\ V_{\mu-2},\dots,\ V_2,\ V_1,\ V_0,$$

dont la dernière V_0 est constante et égale à 2. Trois fonctions consécutives V_n, V_{n-1}, V_{n-2} sont liées entre elles par l'équation

$$(2) \qquad V_n = z\,V_{n-1} - V_{n-2};$$

d'où il suit que :

1°. Deux fonctions consécutives V_n et V_{n-1} ne peuvent s'annuler pour une même valeur de z, puisqu'alors toutes les fonctions suivantes devraient également s'annuler pour la même valeur de z; ce qui est impossible, la dernière étant constante.

2°. Si une fonction V_{n-1} s'annule pour une certaine valeur de z, celle qui la précède et celle qui la suit ont des signes contraires.

Il résulte de là que si l'on fait varier z depuis α jusqu'à 6, la suite des signes des fonctions V ne pourra perdre ni gagner de variations, que lorsque z passera par une valeur qui annule V_μ, et que si la suite des signes des fonctions V perd ou gagne k variations quand z varie de α jusqu'à 6, l'équation (1) a *au moins k* racines comprises entre α et 6.

Cela posé, on déduit aisément de l'équation (2), que l'on a pour $z = -2$,

$$V_0 = +2, \quad V_1 = -2, \quad V_2 = +2, \quad V_3 = -2, \ldots,$$

et, pour $z = +2$,

$$V_0 = +2, \quad V_1 = +2, \quad V_2 = +2, \quad V_3 = +2, \ldots;$$

en sorte que la suite des signes des fonctions V perd μ variations quand z varie de -2 jusqu'à $+2$; d'où il suit que l'équation (1) a ses μ racines réelles et comprises entre -2 et $+2$.

En outre, puisque toutes les racines sont réelles, la suite des signes des fonctions V perdra effectivement une variation chaque fois que z, variant de -2 jusqu'à $+2$, dépassera une racine de l'équation (1), et cette variation se perdra entre les deux premiers termes de la suite, de manière que $V_{\mu-1}$ jouera, par rapport à V_μ, le même rôle que si elle en était la dérivée; ce qui veut dire que les racines de $V_{\mu-1} = 0$ pourront servir à la séparation des racines de $V_\mu = 0$. Enfin, si α et 6 sont deux nombres quelconques compris entre -2 et $+2$, l'équation proposée a autant de racines entre α et 6, qu'il y a d'unités dans l'excès du nombre des variations de signes de la suite des fonctions V pour $z = \alpha$, sur le

nombre des variations de signes de cette suite pour $z = \beta$.

De l'équation $U_\mu = 0$. — Ce qui précède s'applique textuellement à l'équation

$$U_\mu = 0,$$

qui se trouve dans les mêmes conditions que l'équation $V_\mu = 0$.

Si l'on considère la suite des fonctions

$$U_\mu,\ U_{\mu-1},\ U_{\mu-2},\ldots,\ U_2,\ U_1,\ U_0,$$

on voit que la dernière est constante, et l'équation

$$U_n = zU_{n-1} - U_{n-2}$$

conduit facilement à cette conséquence, que la suite des signes des fonctions U ne peut perdre ou gagner de variations quand on fait varier z, que lorsque z atteint et dépasse une valeur qui annule la première de ces fonctions; d'où il suit que l'équation proposée a au moins autant de racines entre α et β qu'il y a de variations perdues ou gagnées dans la suite des signes des fonctions U, quand z varie de α à β.

On trouve, d'ailleurs, que pour $z = -2$, la suite des signes des fonctions U présente μ variations, tandis qu'elle n'en présente aucune pour $z = +2$; d'où l'on conclut que l'équation $U_\mu = 0$ a ses μ racines réelles et comprises entre -2 et $+2$.

On démontre très-simplement, dans les cours d'algèbre élémentaire, la réalité des racines des équations que nous venons de considérer; mais j'ai cru devoir présenter ici la méthode de M. Sturm, parce qu'elle s'applique avec succès dans un grand nombre de cas.

QUATORZIÈME LEÇON.

Formation d'une équation différentielle, linéaire du deuxième ordre, à laquelle satisfait la fonction V_n. — Expression du polynôme V_n. — Expressions de $\cos na$ et de $\frac{\sin na}{\sin a}$ en fonction de $\cos a$. — Expression du polynôme U_n. — Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction U_n. — Nouvelle manière de démontrer la réalité des racines des équations $V_n = 0$, $U_n = 0$.

Je présenterai dans cette leçon quelques développements sur les polynômes V_n et U_n, auxquels nous a conduits la considération de l'équation binôme.

Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction V_n.

V_n est une fonction entière d'une variable z. On a

(1) $$V_n = x^n + \frac{1}{x^n}$$

et

(2) $$z = x + \frac{1}{x},$$

d'où

(3) $$\frac{dz}{dx} = 1 - \frac{1}{x^2}.$$

Différentions l'équation (1) par rapport à x, il vient

$$\frac{dV_n}{dz}\frac{dz}{dx} = \frac{dV_n}{dz}\left(1 - \frac{1}{x^2}\right) = n\left(x^{n-1} - \frac{1}{x^{n+1}}\right),$$

ou

(4) $$\left(x - \frac{1}{x}\right)\frac{dV_n}{dz} = n\left(x^n - \frac{1}{x^n}\right);$$

différentions aussi cette équation (4) par rapport à x, il vient

$$\left(x-\frac{1}{x}\right)\left(1-\frac{1}{x^2}\right)\frac{d^2 V_n}{dz^2}+\left(1+\frac{1}{x^2}\right)\frac{dV_n}{dz}=n^2\left(x^{n-1}+\frac{1}{x^{n+1}}\right),$$

ou, en multipliant par x,

$$(5)\quad \left(x-\frac{1}{x}\right)^2\frac{d^2 V_n}{dz^2}+\left(x+\frac{1}{x}\right)\frac{dV_n}{dz}-n^2\left(x^n+\frac{1}{x^n}\right)=0;$$

mais on a

$$x^n+\frac{1}{x^n}=V_n,\quad x+\frac{1}{x}=z,\quad \left(x-\frac{1}{x}\right)^2=z^2-4;$$

donc l'équation (5) devient

$$(6)\qquad (z^2-4)\frac{d^2 V_n}{dz^2}+z\frac{dV_n}{dz}-n^2 V_n=0.$$

C'est l'équation différentielle que nous voulions obtenir, et qui nous servira à déterminer l'expression du polynôme V_n. Il est aisé de démontrer que V_n, ou le produit de V_n par une constante arbitraire, est la seule fonction entière et rationnelle de z qui puisse satisfaire à l'équation (6). En effet, considérons, au lieu de V_n, la fonction plus générale

$$(7)\qquad \Theta_n=A x^n+\frac{B}{x^n},$$

où A et B sont deux constantes arbitraires. En opérant sur Θ_n, comme nous venons de faire sur V_n, on arrivera à l'équation différentielle

$$(8)\qquad (z^2-4)\frac{d^2\Theta_n}{dz^2}+z\frac{d\Theta_n}{dz}-n^2\Theta_n=0,$$

qui ne diffère de (6) qu'en ce que V_n y est remplacé par Θ_n. Cette équation (8) a évidemment pour intégrale générale

l'équation (7), que l'on peut mettre sous la forme

$$\Theta_n = C\left(x^n + \frac{1}{x^n}\right) + nC'\left(x^n - \frac{1}{x^n}\right),$$

en désignant par C et C′ deux constantes arbitraires.

D'ailleurs $x^n + \frac{1}{x^n}$ est précisément V_n, et l'équation (4) donne

$$x^n - \frac{1}{x^n} = \frac{1}{n}\left(x - \frac{1}{x}\right)\frac{dV_n}{dz} = \frac{1}{n}\sqrt{z^2 - 4}\,\frac{dV_n}{dz},$$

d'où il résulte que l'intégrale générale de l'équation (8) est

$$\Theta_n = CV_n + C'\sqrt{z^2 - 4}\,\frac{dV_n}{dz},$$

C et C′ étant les deux constantes arbitraires; et, par conséquent, le produit de V_n par une constante C est la fonction rationnelle la plus générale qui puisse satisfaire à l'équation (8).

Expression du polynôme V_n.

Nous savons que V_n est un polynôme du degré n en z, qui ne renferme que des termes de même parité que n; nous savons aussi que le terme du plus haut degré a pour coefficient l'unité. Nous poserons donc

$$(1)\quad V_n = z^n + A_1 z^{n-2} + A_2 z^{n-4} + \ldots + A_{p-1} z^{n-2p+2} + A_p z^{n-2p} + \ldots,$$

et nous allons chercher à déterminer les coefficients A_1, A_2, etc., par la condition que V_n satisfasse à l'équation différentielle

$$(2)\qquad (z^2 - 4)\frac{d^2V_n}{dz^2} + z\frac{dV_n}{dz} - n^2V_n = 0.$$

On tire de l'équation (1), par la différentiation,

$$\frac{d\mathrm{V}_n}{dz} = nz^{n-1} + \ldots + (n-2p)\,\mathrm{A}_p\, z^{n-2p-1} + \ldots,$$

$$\frac{d^2\mathrm{V}_n}{dz^2} = n(n-1)z^{n-2} + \ldots + (n-2p+2)(n-2p+1)\,\mathrm{A}_{p-1}\, z^{n-2p}$$
$$+ (n-2p)(n-2p-1)\,\mathrm{A}_p\, z^{n-2p-2} + \ldots,$$

et, en substituant dans l'équation (2) les valeurs de V_n, $\frac{d\mathrm{V}_n}{dz}$, $\frac{d^2\mathrm{V}_n}{dz^2}$, le coefficient de z^{n-2p} sera

$$\left.\begin{array}{r}(n-2p)(n-2p-1)\\ +(n-2p)\\ -n^2\end{array}\right|\mathrm{A}_p - 4(n-2p+2)(n-2p+1)\,\mathrm{A}_{p-1}$$

ou

$$-4p(n-p)\,\mathrm{A}_p - 4(n-2p+2)(n-2p+1)\,\mathrm{A}_{p-1},$$

mais ce coefficient doit être nul, on a donc

$$\mathrm{A}_p = -\frac{(n-2p+2)(n-2p+1)}{p(n-p)}\,\mathrm{A}_{p-1}.$$

Cette relation conduit aisément à l'expression générale de A_p; car, le coefficient A_0 de z^n étant égal à 1, on a

$$\mathrm{A}_p = -\frac{(n-2p+2)(n-2p+1)}{p(n-p)}\,\mathrm{A}_{p-1},$$

$$\mathrm{A}_{p-1} = -\frac{(n-2p+4)(n-2p+3)}{(p-1)(n-p+1)}\,\mathrm{A}_{p-2},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathrm{A}_2 = -\frac{(n-2)(n-3)}{2.(n-2)}\,\mathrm{A}_1,$$

$$\mathrm{A}_1 = -\frac{n(n-1)}{1.(n-1)}.$$

En multipliant toutes ces équations, et supprimant les

facteurs communs, il vient

$$A_p = (-1)^p \frac{n(n-p-1)(n-p-2)\ldots(n-2p+2)(n-2p+1)}{1.2.3\ldots p};$$

la valeur du polynôme V_n est donc

$$(3)\ \begin{cases} V_n = z^n - nz^{n-2} + \dfrac{n(n-3)}{1.2} z^{n-4} - \dfrac{n(n-4)(n-5)}{1.2.3} z^{n-6} + \ldots \\ + (-1)^p \dfrac{n(n-p-1)(n-p-2)\ldots(n-2p+2)(n-2p+1)}{1.2.3\ldots p} z^{n-2p} + \ldots \end{cases}$$

On peut obtenir de diverses manières l'expression du polynôme V_n que nous venons de former. On peut, en particulier, déduire cette expression de la formule qui fait connaître les sommes de puissances semblables des racines de l'équation du second degré, ainsi que cela se trouve expliqué dans la Note I. La méthode que nous avons adoptée ici est fort simple et elle a surtout l'avantage de pouvoir être employée utilement dans un assez grand nombre de questions analogues.

Expressions de $\cos na$ *et de* $\dfrac{\sin na}{\sin a}$ *en fonction de* $\cos a$.

Le problème que nous venons de résoudre est identique à celui qui a pour objet de trouver l'expression de $\cos na$ en fonction de $\cos a$. Si, effet, on pose

$$x = \cos a + \sqrt{-1}\sin a,$$

on a

$$z = 2\cos a,\quad V_n = 2\cos na.$$

Exprimer V_n en fonction de z, c'est donc exprimer $\cos na$ en fonction de $\cos a$. En remplaçant V_n et z par $2\cos na$, et $2\cos a$ dans l'équation que nous avons trouvée, il vient

$$(1)\ \begin{cases} \cos na = 2^{n-1}\cos^n a - 2^{n-3} n \cos^{n-2} a + 2^{n-5} \dfrac{n(n-3)}{1.2} \cos^{n-4} a - \ldots \\ + (-1)^p 2^{n-2p-1} \dfrac{n(n-p-1)(n-p-2)\ldots(n-2p+1)}{1.2.3\ldots p} \cos^{n-2p} a. \end{cases}$$

$\sin na$ n'est jamais exprimable en fonction rationnelle de $\cos a$, mais le rapport $\frac{\sin na}{\sin a}$ l'est toujours. En différentiant l'équation précédente par rapport à a, et divisant ensuite par $-n \sin a$, on a

$$(2)\left\{\begin{aligned}&\frac{\sin na}{\sin a} = 2^{n-1}\cos^{n-1}a - 2^{n-3}(n-2)\cos^{n-3}a + 2^{n-5}\frac{(n-3)(n-4)}{1.2}\cos^{n-5}a - \ldots\\ &+(-1)^p 2^{n-2p-1}\frac{(n-p-1)(n-p-2)\ldots(n-2p+1)(n-2p)}{1.2.3\ldots p}\cos^{n-2p-1}a + .\end{aligned}\right.$$

Enfin, en changeant a en $\frac{\pi}{2} - a$ dans les équations (1) et (2), on aura deux autres formules, qui feront connaître, en fonction rationnelle de $\sin a$, $\cos na$ et $\frac{\sin na}{\cos a}$ si n est pair, $\frac{\cos na}{\cos a}$ et $\sin na$ si n est impair.

Expression du polynôme U_n.

Nous avons trouvé, en différentiant V_n par rapport à x,

$$\left(x - \frac{1}{x}\right)\frac{dV_n}{dz} = n\left(x^n - \frac{1}{x^n}\right),$$

on déduit de là

$$\frac{1}{n}\frac{dV_n}{dz} = \frac{x^n - \frac{1}{x^n}}{x - \frac{1}{x}} = x^{n-1} + x^{n-3} + x^{n-5} + \ldots + \frac{1}{x^{n-3}} + \frac{1}{x^{n-1}};$$

on aurait de même

$$\frac{1}{n+1}\frac{dV_{n+1}}{dz} = x^n + x^{n-2} + x^{n-4} + \ldots + \frac{1}{x^{n-4}} + \frac{1}{x^{n-2}} + \frac{1}{x^n},$$

et, par suite,

$$\frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz} = x^n + x^{n-1} + \ldots + \frac{1}{x^{n-1}} + \frac{1}{x^n};$$

mais le second membre de cette équation est précisément égal à U_n, on a donc

$$U_n = \frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz}.$$

De l'expression précédemment trouvée pour V_n, on tire

$$\frac{1}{n}\frac{dV_n}{dz} = z^{n-1} - (n-2)\,z^{n-3} + \frac{(n-3\,(n-4)}{1.2}\,z^{n-5} - \ldots;$$

on a aussi, en changeant n en $n+1$,

$$\frac{1}{n+1}\frac{dV_{n+1}}{dz} = z^n - (n-1)\,z^{n-2} + \frac{(n-2)(n-3)}{1.2}\,z^{n-4} - \ldots.$$

Par suite, la valeur de U_n sera

$$U_n = z^n + z^{n-1} - (n-1)z^{n-2} - (n-2)z^{n-3} + \frac{(n-2)(n-3)}{1.2}\,z^{n-4}$$
$$+ \frac{(n-3)(n-4)}{1.2}\,z^{n-5} - \ldots + (-1)^p\frac{(n-p)\ldots(n-2p+1)}{1.2\ldots p}\,z^{n-2p}$$
$$+ (-1)^p\frac{(n-p-1)\ldots(n-2p)}{1.2\ldots p}\,z^{n-2p-1} + \ldots.$$

Dans cette expression, les termes de même parité que n proviennent tous de $\frac{dV_{n+1}}{dz}$, les autres proviennent de $\frac{dV_n}{dz}$.

Formation d'une équation différentielle linéaire du deuxième ordre, à laquelle satisfait la fonction U_n.

On pourrait employer, pour déterminer le polynôme U_n, un procédé semblable à celui dont nous nous sommes servi pour calculer V_n; on formerait ainsi une équation différentielle à laquelle satisferait U_n, et dont on déduirait ensuite la valeur de ce polynôme; cette seconde marche, que je me borne à indiquer, est beaucoup moins

simple que celle que nous avons suivie, mais l'équation différentielle dont nous venons de parler est utile à connaître. Voici, je crois, le moyen le plus aisé de la trouver.

On a

$$U_n = \left(x^n + \frac{1}{x^n}\right) + \left(x^{n-1} + \frac{1}{x^{n-1}}\right) + \ldots + \left(x + \frac{1}{x}\right) + 1,$$

d'où, en différentiant par rapport à x, se rappelant que $\frac{dz}{dx} = 1 - \frac{1}{x^2}$, et multipliant ensuite par x,

$$\left(x - \frac{1}{x}\right)\frac{dU_n}{dz} = n\left(x^n - \frac{1}{x^n}\right) + (n-1)\left(x^{n-1} - \frac{1}{x^{n-1}}\right) + \ldots + \left(x - \frac{1}{x}\right);$$

multipliant par $x - \frac{1}{x}$, et observant que

$$\left(x - \frac{1}{x}\right)^2 = z^2 - 4 \quad \text{et} \quad \left(x^p - \frac{1}{x^p}\right)\left(x - \frac{1}{x}\right) = V_{p+1} - V_{p-1},$$

il vient

$$\begin{aligned}(z^2 - 4)\frac{dU_n}{dz} &= n(V_{n+1} - V_{n-1}) + (n-1)(V_n - V_{n-2}) \ldots \\ &\quad + 3(V_4 - V_2) + 2(V_3 - V_1) + (V_2 - 2) \\ &= nV_{n+1} + (n+1)V_n - 2(V_n + V_{n-1} + \ldots + V_2 + V_1 + 1),\end{aligned}$$

ou

$$(z^2 - 4)\frac{dU_n}{dz} + 2U_n = nV_{n+1} + (n+1)V_n.$$

Différentiant cette équation par rapport à z, on obtient

$$(z^2 - 4)\frac{d^2U_n}{dz^2} + 2(z+1)\frac{dU_n}{dz} = n(n+1)\left(\frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz}\right).$$

Mais nous avons déjà trouvé

$$U_n = \frac{1}{n}\frac{dV_n}{dz} + \frac{1}{n+1}\frac{dV_{n+1}}{dz};$$

on a donc enfin

$$(1)\quad (z^2-4)\frac{d^2 U_n}{dz^2}+2(z+1)\frac{dU_n}{dz}-n(n+1)U_n=0.$$

C'est l'équation différentielle que nous voulions former.

Il suit de là que l'équation

$$(2)\quad (z^2-4)\frac{d^2 \Theta_n}{dz^2}+2(z+1)\frac{d\Theta_n}{dz}-n(n+1)\Theta_n=0$$

est satisfaite par

$$\Theta_n = U_n,\quad \text{ou}\quad \Theta_n = CU_n,$$

C désignant une constante arbitraire; et cette solution CU_n est la seule solution rationnelle de l'équation (2). On s'en assure aisément en cherchant l'intégrale générale de l'équation (2), qui est

$$\Theta_n = CU_n + C'\sqrt{\frac{z+2}{z-2}}\left[U_n + 2(z-2)\frac{dU_n}{dz}\right],$$

C et C′ désignant deux constantes arbitraires; on voit que cette valeur de Θ_n n'est rationnelle que si l'on fait $C'=0$, auquel cas elle se réduit à CU_n.

Nouvelle manière de démontrer la réalité des racines des équations $V_n=0$, $U_n=0$.

Les deux équations différentielles que nous avons formées et auxquelles satisfont les fonctions V_n et U_n, permettent de démontrer la réalité des racines des équations

$$V_n=0,\quad U_n=0.$$

Cette remarque est importante, car un procédé analogue pourra être employé dans beaucoup d'autres cas. Nous ne nous occuperons que de l'équation $V_n=0$; les mêmes considérations s'appliqueraient à l'équation $U_n=0$.

Nous avons trouvé l'équation différentielle

$$(1)\qquad (z^2-4)\frac{d^2 V_n}{dz^2}+z\frac{dV_n}{dz}-n^2V_n=0;$$

différentions $p-2$ fois cette équation, et observons que

$$\frac{d^{p-2}}{dz^{p-2}}(z^2-4)\frac{d^2 V_n}{dz^2} = (z^2-4)\frac{d^p V_n}{dz^p} + 2(p-2)z\frac{d^{p-1} V_n}{dz^{p-1}} + (p-2)(p-3)\frac{d^{p-2} V_n}{dz^{p-2}},$$

$$\frac{d^{p-2}}{dz^{p-2}} z\frac{dV_n}{dz} = z\frac{d^{p-1} V_n}{dz^{p-1}} + (p-2)\frac{d^{p-2} V_n}{dz^{p-2}},$$

on aura

$$(2)\qquad \left\{ (z^2-4)\frac{d^p V_n}{dz^p} + (2p-3)z\frac{d^{p-1} V_n}{dz^{p-1}} - [n^2-(p-2)^2]\frac{d^{p-2} V_n}{dz^{p-2}} = 0. \right.$$

Les équations (1) et (2) peuvent s'écrire ainsi :

$$(3)\qquad \left\{ \begin{aligned} V_n &= z\frac{dV_n}{dz} - (4-z^2)\frac{d^2 V_n}{dz^2}, \\ \frac{d^{p-2} V_n}{dz^{p-2}} &= \frac{2p-3}{n^2-(p-2)^2}\, z\frac{d^{p-1} V_n}{dz^{p-1}} - \frac{4-z^2}{n^2-(p-2)^2}\frac{d^p V_n}{dz^p}. \end{aligned} \right.$$

Cela posé, considérons la suite formée de la fonction V_n et de toutes ses dérivées, savoir :

$$(4)\qquad V_n,\quad \frac{dV_n}{dz},\quad \frac{d^2 V_n}{dz^2},\ldots,\quad \frac{d^n V_n}{dz^n};$$

la dernière de ces fonctions est constante. On voit, en outre, par les équations (3), que :

1°. Deux fonctions consécutives ne peuvent s'annuler pour une même valeur de z comprise entre -2 et $+2$; car alors toutes les suivantes s'annuleraient pour cette valeur de z, ce qui est impossible, la dernière étant une constante différente de zéro.

2°. Si une fonction s'annule pour une valeur de z comprise entre -2 et $+2$, la fonction qui la précède et celle

qui la suit sont de signes contraires pour cette même valeur de z.

Il résulte de là que, si l'on veut appliquer la méthode de M. Sturm à l'équation

$$V_n = 0, \tag{5}$$

on pourra substituer la suite (4) à la suite des fonctions que l'on obtiendrait en exécutant sur V_n et sa dérivée l'opération du plus grand commun diviseur, avec la précaution qu'exige la méthode relativement au changement de signe des restes; pourvu qu'on ne fasse varier z que de -2 à $+2$. Et si α et 6 désignent deux nombres quelconques compris entre -2 et $+2$, tels que $\alpha < 6$, l'équation (5) aura autant de racines comprises entre α et 6 qu'il y aura d'unités dans l'excès du nombre des variations des signes de la suite (4) pour $z = \alpha$, sur le nombre des variations des signes de cette suite pour $z = 6$.

Faisons d'abord $z = -2$, les équations (3) donneront

$$V_n = -2\frac{dV_n}{dz}, \quad \frac{d^{p-2}V_n}{dz^{p-2}} = -2\frac{2p-3}{n^2-(p-2)^2}\frac{d^{p-1}V_n}{dz^{p-1}};$$

et, par conséquent, la suite (4) présente n variations de signes pour $z = -2$.

Faisons ensuite $z = +2$; les équations (3) donneront

$$V_n = 2\frac{dV_n}{dz}, \quad \frac{d^{p-2}V_n}{dz^{p-2}} = 2\frac{2p-3}{n^2-(p-2)^2}\frac{d^{p-1}V}{dz^{p-1}},$$

et, par conséquent, la suite (4) ne présente aucune variation pour $z = 2$.

Donc, enfin, les n racines de l'équation (5) sont réelles et comprises entre -2 et $+2$.

QUINZIÈME LEÇON.

Résolution de l'équation générale du troisième degré. — Méthode de Hudde. — Méthode de Lagrange. — Comparaison des deux méthodes précédentes. — Méthode de Tschirnaüs. — Méthode d'Euler.

Résolution de l'équation générale du troisième degré.

Je me propose, dans cette leçon, d'exposer les principales méthodes connues pour la résolution des équations du troisième degré.

Méthode de Hudde.

Des diverses méthodes connues pour la résolution de l'équation générale du troisième degré, la plus simple est, sans contredit, celle de Hudde. C'est aussi celle que nous exposerons la première.

Comme on peut toujours faire disparaître le second terme d'une équation, nous considérerons l'équation

$$(1) \qquad x^3 + px + q = 0$$

débarrassée du terme en x^2. Posons

$$(2) \qquad x = y + z,$$

y étant une nouvelle variable et z une fonction de y, que nous nous réservons de déterminer, de manière que l'équation transformée en y rentre, s'il est possible, dans les classes d'équations que nous savons résoudre. Remplaçons dans l'équation (1) x par sa valeur tirée de (2), on aura

$$(y+z)^3 + p(y+z) + q = 0,$$

ou

$$(3)\qquad (y^3 + z^3 + q) + (y + z)(3yz + p) = 0.$$

Si, maintenant, on détermine z par la condition

$$3yz + p = 0,$$

on a

$$z = -\frac{p}{3y};$$

et l'équation (3) se réduit à

$$y^3 - \frac{p^3}{27y^3} + q = 0,$$

ou

$$(4)\qquad y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Cette équation en y peut se résoudre à la manière des équations du second degré, car elle ne contient que les puissances y^3 et y^6. Ensuite, quand y sera connu, on aura x par la formule

$$(5)\qquad x = y - \frac{p}{3y}.$$

L'équation du sixième degré (4), à laquelle nous ramenons ainsi l'équation proposée, a été appelée par Lagrange la *réduite* ou *résolvante* de l'équation (1).

Quoique cette résolvante ait six racines, la formule (5) ne donnera pourtant que trois valeurs de x, comme cela doit être. En effet, la résolvante ne change pas quand on change y en $-\frac{p}{3y}$, en sorte que ses six racines forment trois groupes tels, que le produit des deux racines de chaque groupe est égal à $-\frac{p}{3}$, et il est évident que la formule (5) donnera la même valeur pour x quand on remplacera y successivement par les deux racines d'un même

groupe. Ceci va résulter, au surplus, de l'expression même des valeurs de x dont nous allons nous occuper.

De l'équation (4) on tire cette valeur de y^3,

$$y^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

ou

$$(6) \qquad y^3 = -\frac{q}{2} \pm \sqrt{R},$$

en faisant, pour abréger,

$$R = \frac{q^2}{4} + \frac{p^3}{27}:$$

enfin, l'équation (6) donnera

$$(7) \qquad y = \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Cette expression, à cause des valeurs multiples des radicaux, représente bien les six racines de l'équation (4); mais nous admettrons, dans ce qui va suivre, que $\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}$ représentera seulement l'une des trois racines cubiques de $-\frac{q}{2} \pm \sqrt{R}$. Ce sera celle que l'on voudra, mais ce sera toujours la même; en sorte que, si α et 6 désignent les deux racines cubiques imaginaires de l'unité, les six racines de l'équation (4) pourront être représentées par

$$(8) \quad \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}, \quad \alpha\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}, \quad 6\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Et comme des deux radicaux

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}}, \quad \sqrt[3]{-\frac{q}{2} - \sqrt{R}},$$

le premier nous représente, par notre convention, celle

des trois racines cubiques de $-\frac{q}{2}+\sqrt{R}$ que nous voudrons, le second également celle des trois racines cubiques de $-\frac{q}{2}-\sqrt{R}$ que nous voudrons, et qu'en outre, leur produit a pour cube $-\frac{p^3}{27}$, nous pouvons choisir les valeurs de ces deux radicaux de manière que leur produit soit égal à $-\frac{p}{3}$; on aura alors

$$(9) \qquad \sqrt[3]{-\frac{q}{2}\mp\sqrt{R}}=\frac{-p}{3\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}}}.$$

Si maintenant on porte, dans l'équation (5), chacune des valeurs (8) de y, on aura, en se servant de l'équation (9) et se rappelant que $\alpha\beta=1$, les valeurs suivantes de x :

$$\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}}+\sqrt[3]{-\frac{q}{2}\mp\sqrt{R}},$$

$$\alpha\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}}+\beta\sqrt[3]{-\frac{q}{2}\mp\sqrt{R}},$$

$$\beta\sqrt[3]{-\frac{q}{2}\pm\sqrt{R}}+\alpha\sqrt[3]{-\frac{q}{2}\mp\sqrt{R}},$$

qui se réduisent évidemment à trois distinctes, savoir :

$$\sqrt[3]{-\frac{q}{2}+\sqrt{R}}+\sqrt[3]{-\frac{q}{2}-\sqrt{R}},$$

$$\alpha\sqrt[3]{-\frac{q}{2}+\sqrt{R}}+\beta\sqrt[3]{-\frac{q}{2}-\sqrt{R}},$$

$$\beta\sqrt[3]{-\frac{q}{2}+\sqrt{R}}+\alpha\sqrt[3]{-\frac{q}{2}-\sqrt{R}}.$$

Ces trois racines de l'équation (1) pourront être représentées par la formule unique

$$(10)\qquad x=\sqrt[3]{-\frac{q}{2}+\sqrt{R}}+\sqrt[3]{-\frac{q}{2}-\sqrt{R}},$$

dite *formule de Cardan*, pourvu qu'alors on laisse aux radicaux cubiques toute leur généralité, mais qu'on n'associe ensemble que les valeurs de ces radicaux qui donnent un produit égal à $-\frac{p}{3}$.

Si, dans la formule (10), on combine chaque valeur du premier radical cubique avec chaque valeur du second, on aura en tout neuf valeurs de x, qui seront les racines des trois équations

$$x^3+px\;\;+q=0,$$
$$x^3+p\alpha x+q=0,$$
$$x^3+p6x+q=0,$$

ainsi qu'on s'en assure aisément en faisant disparaître les radicaux de l'équation (10).

Tout ce qui précède a lieu, quelles que soient les quantités p et q, réelles ou imaginaires. Nous allons ajouter quelques détails relatifs seulement au cas où les coefficients sont réels.

Discussion de la formule de Cardan. — p et q étant réels, supposons $R>0$, ou

$$4p^3+27q^2>0;$$

les deux radicaux qui entrent dans l'équation (10) auront chacun une de leurs trois valeurs réelles. Désignons par A la valeur réelle du premier, par B celle du second, les trois valeurs du premier radical seront

$$A,\quad A\alpha,\quad A6,$$

celles du second seront

$$B,\ B\alpha,\ B\beta;$$

et comme les valeurs des deux radicaux, qu'il faut prendre ensemble, doivent avoir un produit réel, on aura, pour les racines de l'équation (1),

$$A+B,$$
$$A\alpha+B\beta,$$
$$A\beta+B\alpha.$$

D'ailleurs,

$$\alpha=\frac{-1+\sqrt{-3}}{2},\qquad \beta=\frac{-1-\sqrt{-3}}{2};$$

les trois racines de l'équation (1) seront donc

$$A+B \quad \text{et} \quad -\frac{A+B}{2}\pm\frac{A-B}{2}\sqrt{-3}.$$

Ainsi, dans ce cas, l'équation (1) a deux racines imaginaires.

Si l'on a $R=0$, ou

$$4p^3+27q^2=0,$$

la seule différence avec le cas précédent est que l'on a ici $B=A$; alors l'équation (1) a ses trois racines réelles, mais deux sont égales entre elles.

Supposons, en troisième lieu, $R<0$, ou

$$4p^3+27q^2<0,$$

chacun des radicaux qui entrent dans la valeur de x aura ses trois valeurs imaginaires; mais il est facile de voir que l'équation (1) a ses racines réelles et inégales. Soient, en effet,

$$A+B\sqrt{-1},\quad \alpha\left(A+B\sqrt{-1}\right),\quad \beta\left(A+B\sqrt{-1}\right),$$

les trois racines cubiques de l'expression imaginaire $-\frac{q}{2}+\sqrt{R}$; l'expression imaginaire conjuguée $-\frac{q}{2}-\sqrt{R}$ aura évidemment pour racines cubiques

$$A-B\sqrt{-1},\quad 6(A-B\sqrt{-1}),\quad \alpha(A-B\sqrt{-1});$$

et comme les valeurs des deux radicaux qui forment la valeur (10) de x doivent avoir un produit réel, on aura les trois valeurs suivantes de x :

$$\begin{gathered}(A+B\sqrt{-1})+\ (A-B\sqrt{-1}),\\ \alpha(A+B\sqrt{-1})+6(A-B\sqrt{-1}),\\ 6(A+B\sqrt{-1})+\alpha(A-B\sqrt{-1});\end{gathered}$$

ou, en remplaçant α et 6 par leurs valeurs,

$$2A,\quad -A+B\sqrt{3},\quad -A-B\sqrt{3}.$$

L'équation (1) a donc ses trois racines réelles, comme nous l'avions annoncé, et il est très-facile de montrer qu'elles sont inégales.

En effet, on ne peut avoir d'abord

$$-A+B\sqrt{3}=-A-B\sqrt{3},$$

car il en résulterait $B=0$, et la quantité $-\frac{q}{2}+\sqrt{R}$ serait égale à la quantité réelle A^3, ce qui est contre l'hypothèse. On ne peut avoir non plus

$$2A=-A\pm B\sqrt{3},$$

car il en résulterait $B=\pm A\sqrt{3}$; par suite,

$$A+B\sqrt{-1}=A(1\pm\sqrt{-3})=-2\alpha A,$$

et

$$-\frac{q}{2}+\sqrt{R}=-8\alpha^3 A^3=-8A^3,$$

ce qui est encore contre l'hypothèse, puisque le second membre est réel.

Le cas que nous avons examiné en dernier lieu est fort remarquable; car, bien qu'alors les trois racines de l'équation du troisième degré soient réelles, la formule de Cardan présente leurs valeurs sous une forme compliquée d'imaginaires : et si, pour faire disparaître ces imaginaires, on cherchait à mettre les radicaux cubiques qui entrent dans la formule de Cardan sous la forme $A+B\sqrt{-1}$, on trouverait que les quantités A et B dépendent d'une équation toute semblable à la proposée. L'équation en A, par exemple, aurait ses trois racines réelles, et l'on trouverait, par conséquent, une expression de A également compliquée d'imaginaires. C'est pour cette raison que le cas dont il s'agit ici a été nommé le *cas irréductible*.

La formule de Cardan ne peut donc servir à la résolution *numérique* de l'équation du troisième degré que si une seule racine est réelle. Mais dans le cas irréductible, l'équation se résout très-simplement en faisant usage des lignes trigonométriques. Si l'on pose, en effet,

$$\frac{q^2}{4}+\frac{p^3}{27}=-\rho^2\sin^2\omega,\quad -\frac{q}{2}=\rho\cos\omega,$$

la quantité ρ et l'angle ω se trouveront déterminés par les formules

$$\rho=\sqrt{\frac{-p^3}{27}},\quad \cos\omega=\frac{\frac{-q}{2}}{\sqrt{\frac{-p^3}{27}}},$$

et la formule de Cardan donnera

$$x = \sqrt[3]{\rho}\left(\sqrt[3]{\cos\omega + \sqrt{-1}\sin\omega} + \sqrt[3]{\cos\omega - \sqrt{-1}\sin\omega}\right),$$

$\sqrt[3]{\rho}$ désignant une quantité réelle. On a d'ailleurs

$$\sqrt[3]{\cos\omega + \sqrt{-1}\sin\omega} = \cos\frac{\omega + 2k\pi}{3} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

$$\sqrt[3]{\cos\omega - \sqrt{-1}\sin\omega} = \cos\frac{\omega + 2k\pi}{3} - \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

où k a l'une des trois valeurs 0, 1, 2. On doit donner à k la même valeur dans ces deux formules, car il faut que le produit de leurs premiers membres soit réel ; on aura donc

$$x = 2\sqrt[3]{\rho}\cos\frac{\omega + 2k\pi}{3},$$

et les trois racines de l'équation seront

$$2\sqrt[3]{\rho}\cos\frac{\omega}{3},\quad 2\sqrt[3]{\rho}\cos\frac{\omega + 2\pi}{3},\quad 2\sqrt[3]{\rho}\cos\frac{\omega + 4\pi}{3}.$$

On pourra, dans chaque cas, calculer par logarithmes les trois racines dont nous venons de donner l'expression.

Méthode de Lagrange.

Considérons l'équation complète du troisième degré

$$(1)\qquad x^3 + Px^2 + Qx + R = 0,$$

et désignons par x_1, x_2, x_3 ses trois racines. D'après la théorie exposée dans les onzième et douzième leçons, on pourra déterminer les valeurs des racines x_1, x_2, x_3, si l'on parvient à connaître la valeur d'une fonction quelconque de ces racines, tellement choisie cependant, que les six valeurs qu'elle peut prendre par les 1.2.3 permutations des lettres x_1, x_2, x_3 soient différentes. La méthode

de Lagrange, que nous allons exposer ici, consiste à déterminer directement la valeur d'une fonction linéaire des trois racines, telle que

$$(2) \qquad t = x_1 + Ax_2 + Bx_3,$$

où A et B désignent des constantes quelconques, et à déduire ensuite de cette fonction l'expression des racines elles-mêmes.

Si l'on fait subir aux lettres x_1, x_2, x_3 toutes les permutations possibles, on aura les six valeurs suivantes de la fonction t :

$$(3) \quad \begin{cases} t_1 = x_1 + Ax_2 + Bx_3, \\ t_2 = x_1 + Ax_3 + Bx_2, \\ t_3 = x_2 + Ax_3 + Bx_1, \\ t_4 = x_2 + Ax_1 + Bx_3, \\ t_5 = x_3 + Ax_1 + Bx_2, \\ t_6 = x_3 + Ax_2 + Bx_1, \end{cases}$$

et cette fonction t dépendra de l'équation du sixième degré

$$(4) \quad (t - t_1)(t - t_2)(t - t_3)(t - t_4)(t - t_5)(t - t_6) = 0,$$

qui pourra être résolue à la manière des équations du second degré, si l'on peut disposer des constantes indéterminées A et B, de façon qu'elle ne renferme que la sixième et la troisième puissance de t. Il faut et il suffit, pour qu'il en soit ainsi, que, t désignant l'une quelconque des racines de l'équation (4), α une racine cubique imaginaire de l'unité, αt et $\alpha^2 t$ soient aussi racines de l'équation (4). Voyons si cette condition peut être remplie. D'abord αt_1 et $\alpha^2 t_1$ ne peuvent être égaux ni à t_2, ni à t_4, ni à t_6, car autrement on aurait $\alpha = 1$; il faut donc que l'on ait

$$\alpha t_1 = t_3 \quad \text{et} \quad \alpha^2 t_1 = t_5,$$

ou

$$\alpha t_1 = t_5 \quad \text{et} \quad \alpha^2 t_1 = t_3.$$

Ces deux dernières équations équivalent aux précédentes, puisque rien ne distingue les racines α et α^2 l'une de l'autre; nous adopterons les dernières, et comme elles doivent avoir lieu, quelles que soient x_1, x_2, x_3, nous en déduirons les valeurs suivantes de A et B,

$$A = \alpha, \quad B = \alpha^2.$$

Il arrive alors que A et B ayant ces valeurs, on a aussi

$$\alpha t_2 = t_4, \quad \alpha^2 t_2 = t_6,$$

en sorte que si l'on prend pour valeur de t

$$t = x_1 + \alpha x_2 + \alpha^2 x_3,$$

l'équation en t aura pour racines

$$t_1, \ \alpha t_1, \ \alpha^2 t_1, \ t_2, \ \alpha t_2, \ \alpha^2 t_2,$$

et sera, par conséquent,

$$(t^3 - t_1^3)(t^3 - t_2^3) = 0,$$

ou

(5) $$t^6 - (t_1^3 + t_2^3)t^3 + t_1^3 t_2^3 = 0,$$

en faisant

(6) $$\begin{cases} t_1 = x_1 + \alpha x_2 + \alpha^2 x_3, \\ t_2 = x_1 + \alpha^2 x_2 + \alpha x_3. \end{cases}$$

Lorsque les valeurs de t_1 et t_2 seront connues, celles de x_1, x_2, x_3 le seront aisément; on a, en effet,

(7) $$-P = x_1 + x_2 + x_3,$$

et en ajoutant les équations (6) et (7), il vient, à cause de $\alpha^2 + \alpha + 1 = 0$,

(8) $$x_1 = \frac{-P + t_1 + t_2}{3}.$$

14.

Pour avoir x_2, il faut ajouter les trois équations (6) et (7), après les avoir multipliées respectivement par α^2, α et 1; on a ainsi

(9) $$x_2 = \frac{-P + \alpha^2 t_1 + \alpha t_2}{3},$$

et enfin on obtient la valeur suivante de x_3,

(10) $$x_3 = \frac{-P + \alpha t_1 + \alpha^2 t_2}{3},$$

en ajoutant les équations (6) et (7), après les avoir respectivement multipliées par α, α^2 et 1.

Tout est donc ramené à résoudre l'équation (5), qui est alors une *réduite* ou une *résolvante* de l'équation proposée. Cherchons d'abord à exprimer les coefficients de la résolvante par ceux de l'équation proposée, ce qui est possible, puisque ces coefficients $t_1^3 + t_2^3$ et $t_1^3 t_2^3$ sont des fonctions symétriques des racines de l'équation proposée.

Si l'on multiplie les deux équations (6), et qu'on ait égard à la relation $\alpha^2 + \alpha + 1 = 0$, il vient

$$\begin{aligned} t_1 t_2 &= x_1^2 + x_2^2 + x_3^2 - x_1 x_2 - x_1 x_3 - x_2 x_3, \\ &= (x_1 + x_2 + x_3)^2 - 3(x_1 x_2 + x_1 x_3 + x_2 x_3); \end{aligned}$$

et, par conséquent,

(11) $$t_1 t_2 = P^2 - 3Q;$$

si, enfin, on ajoute les deux équations (6), après les avoir élevées au cube, on a

$$\begin{aligned} t_1^3 + t_2^3 &= 2(x_1^3 + x_2^3 + x_3^3) \\ &- 3(x_1^2 x_2 + x_2^2 x_1 + x_1^2 x_3 + x_3^2 x_1 + x_2^2 x_3 + x_3^2 x_2) + 12 x_1 x_2 x_3 \\ &= 3(x_1^3 + x_2^3 + x_3^3) - (x_1 + x_2 + x_3)^3 + 18 x_1 x_2 x_3 \\ &= -2P^3 + 9PQ - 27R; \end{aligned}$$

la résolvante (5) devient donc

$$t^6 - (-2P^3 + 9PQ - 27R)t^3 + (P^2 - 3Q)^3 = 0.$$

En posant

$$t^3 = \theta,$$

elle se réduit à l'équation du second degré

$$\theta^2 - (-2P^3 + 9PQ - 27R)\theta + (P^2 - 3Q)^3 = 0;$$

et, en appelant θ_1 et θ_2 les deux racines de cette équation, on doit faire

$$t_1 = \sqrt[3]{\theta_1}, \quad t_2 = \sqrt[3]{\theta_2}.$$

Les équations (8), (9) et (10) deviennent alors

$$x_1 = \frac{-P + \sqrt[3]{\theta_1} + \sqrt[3]{\theta_2}}{3},$$

$$x_2 = \frac{-P + \alpha^2\sqrt[3]{\theta_1} + \alpha\sqrt[3]{\theta_2}}{3},$$

$$x_3 = \frac{-P + \alpha\sqrt[3]{\theta_1} + \alpha^2\sqrt[3]{\theta_2}}{3};$$

on prendra pour $\sqrt[3]{\theta_1}$ l'une quelconque des trois valeurs de ce radical, mais la même dans les trois formules : quant à l'autre radical $\sqrt[3]{\theta_2}$, sa valeur est déterminée quand on a fixé celle de $\sqrt[3]{\theta_1}$, car l'équation (11) nous donne

$$\sqrt[3]{\theta_1}.\sqrt[3]{\theta_2} = P^2 - 3Q.$$

Il suit de là que les trois racines pourront être représentées par la formule unique

$$x = \frac{-P + \sqrt[3]{\theta_1} + \sqrt[3]{\theta_2}}{3},$$

qui n'a que trois valeurs distinctes, si l'on considère que $\sqrt[3]{\theta_2}$ y est mis, pour abréger, à la place de $\frac{P^2 - 3Q}{\sqrt[3]{\theta_1}}$.

Comparaison des deux méthodes précédentes.

La méthode de Lagrange, que nous venons d'exposer, est moins simple que celle de Hudde; mais elle est plus directe. Toutefois ces deux méthodes fournissent la même résolvante, et nous allons voir qu'on est naturellement conduit à la méthode de Lagrange, en étudiant à fond celle de Hudde.

Reprenons l'équation générale du troisième degré

(1) $$x^3 + Px^2 + Qx + R = 0.$$

Pour appliquer la méthode de Hudde, on commence par faire disparaître le second terme, en posant

$$x = -\frac{P}{3} + x',$$

ce qui ramène l'équation à la forme

(2) $$x'^3 + px' + q = 0;$$

on pose ensuite

$$x' = y - \frac{p}{3y},$$

et l'on obtient enfin cette résolvante

(3) $$y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Cela posé, si y_1 désigne l'une des trois racines cubiques de $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, y_2 celle des trois racines

cubiques de $-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$, qui, multipliée par y_1, donne pour produit $\frac{-p}{3}$, les six racines de l'équation (3) sont

$$y_1,\quad \alpha y_1,\quad \alpha^2 y_1,\quad y_2,\quad \alpha y_2,\quad \alpha^2 y_2,$$

et celles de l'équation (2)

$$y_1+y_2,\quad \alpha y_1+\alpha^2 y_2,\quad \alpha^2 y_1+\alpha y_2;$$

par suite, en appelant x_1, x_2, x_3 les trois racines de l'équation (1), on a

$$x_1 = -\frac{P}{3}+y_1+y_2,$$

$$x_2 = -\frac{P}{3}+\alpha^2 y_1+\alpha y_2,$$

$$x_3 = -\frac{P}{3}+\alpha y_1+\alpha^2 y_2.$$

Si l'on ajoute ces équations, après les avoir respectivement multipliées d'abord par 1, α, α^2, puis ensuite par 1, α^2, α, il vient

$$y_1 = \frac{x_1+\alpha x_2+\alpha^2 x_3}{3},$$

$$y_2 = \frac{x_1+\alpha^2 x_2+\alpha x_3}{3}.$$

On voit par là que la méthode de Hudde revient, au fond, à former une résolvante en y dont la racine ait pour valeur

$$y = \frac{x_1+\alpha x_2+\alpha^2 x_3}{3},$$

et que cette résolvante ne diffère de celle de Lagrange que par le facteur 3 qui divise les racines.

Méthode de Tschirnaüs.

Nous avons déjà eu l'occasion de mentionner la méthode générale de Tschirnaüs, pour faire disparaître d'une équation autant de termes que l'on veut. Il en résulte une méthode pour la résolution des équations du troisième degré, ainsi que nous en avons déjà fait la remarque. Les calculs qu'exige l'application de cette méthode sont plus simples, si l'on a la précaution de débarrasser d'abord l'équation proposée de son second terme.

Soit l'équation

$$(1) \qquad x^3 + px + q = 0,$$

et posons, conformément à la méthode de Tschirnaüs,

$$(2) \qquad y = a + bx + x^2.$$

Si l'on élimine x entre les équations (1) et (2), on obtiendra cette équation en y,

$$(3) \qquad y^3 + Ay^2 + By + C = 0,$$

où l'on fait, pour abréger,

$$A = -3a + 2p,$$
$$B = 3a^2 - 4pa + pb^2 + 3qb + p^2,$$
$$C = -a^3 + 2pa^2 - p^2a - pb^2a - 3qba + qb^3 + pqb - q^2.$$

Quant à la valeur de x en fonction de y, on peut la calculer au moyen de la formule

$$(4) \qquad x = \frac{dy}{db} = -\frac{y^2\frac{dA}{db} + y\frac{dB}{db} + C\frac{dC}{db}}{3y^2 + 2Ay + B},$$

ainsi qu'on l'a vu dans la huitième leçon.

Enfin, on déterminera a et b de manière que l'on ait

$$A = 0, \quad B = 0.$$

Comme ces équations sont, l'une du second degré, l'autre du premier degré entre a et b, on trouvera facilement les valeurs de a et b; l'équation (3) donnera alors

$$y = \sqrt[3]{-C},$$

et l'équation (4) fera connaître ensuite les trois valeurs de x.

Cette méthode, fort simple au point de vue théorique, conduit à des calculs très-laborieux.

Méthode d'Euler.

Nous nous bornerons à mentionner cette méthode, qui rentre, au fond, dans celle de Tschirnaüs. Elle consiste à éliminer y entre deux équations de la forme

$$ay^2 + by + c = x, \quad y^3 = d,$$

et à identifier l'équation finale en x avec l'équation proposée, dont la résolution s'ensuivra évidemment. On peut disposer, à volonté, de la valeur de l'une des indéterminées a, b, c, d; on peut faire, par exemple, $a = 1$ ou $d = 1$.

SEIZIÈME LEÇON.

Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième et des quantités connnes.— Étude d'une classe étendue d'équations numériqnes du troisième degré, qui possèdent une propriété remarquable.

Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième et des quantités connues.

Considérons l'équation du troisième degré débarrassée du second terme

$$x^3 + px + q = 0, \tag{1}$$

et dans laquelle p et q désignent des fonctions rationnelles de quantités quelconques qu'on regarde comme connues. On peut, comme on va voir, exprimer, dans un cas assez étendu, deux quelconques des trois racines de l'équation (1) en fonction rationnelle de la troisième et des quantités connues.

Désignons par y et z deux quantités ayant pour produit $-\frac{p}{3}$, et dont les cubes ont respectivement pour valeurs

$$\left\{\begin{aligned} y^3 &= -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \\ z^3 &= -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}; \end{aligned}\right. \tag{2}$$

soient aussi α et β les deux racines cubiques imaginaires de l'unité : les trois racines x, x_1, x_2 de l'équation (1) ont

pour valeurs

$$(3)\qquad \begin{cases} x = y + z, \\ x_1 = \alpha y + 6 z, \\ x_2 = 6 y + \alpha z, \end{cases}$$

ainsi qu'on l'a vu dans la dernière leçon; on a d'ailleurs

$$\alpha = \frac{-1 + \sqrt{-3}}{2}, \quad 6 = \frac{-1 - \sqrt{-3}}{2};$$

par suite, les valeurs de x_1 et x_2 deviennent

$$(4)\qquad \begin{cases} x_1 = -\frac{y+z}{2} + \frac{y-z}{2}\sqrt{-3}, \\ x_2 = -\frac{y+z}{2} - \frac{y-z}{2}\sqrt{-3}, \end{cases}$$

ou, à cause de la première des équations (3),

$$(5)\qquad \begin{cases} x_1 = -\frac{x}{2} + \frac{y-z}{2}\sqrt{-3}, \\ x_2 = -\frac{x}{2} - \frac{y-z}{2}\sqrt{-3}. \end{cases}$$

On voit, par là, que x_1 et x_2 sont exprimables en fonction rationnelle de x et des quantités connues, si la quantité $y - z\sqrt{-3}$ l'est elle-même.

On a, par les équations (2),

$$y^3 + z^3 = -q, \quad y^3 - z^3 = \sqrt{q^2 + \frac{4p^3}{27}},$$

et, par hypothèse,

$$yz = -\frac{p}{3};$$

d'ailleurs

$$y - z = \frac{y^3 - z^3}{y^2 + yz + z^2} = \frac{y^3 - z^3}{(y+z)^2 - yz},$$

donc

$$y - z = \frac{\sqrt{q^2 + \frac{4p^3}{27}}}{x^2 + \frac{p}{3}};$$

portant cette valeur de $y - z$ dans les équations (5), il vient

$$x_1 = -\frac{x}{2} + \frac{\sqrt{-4p^3 - 27q^2}}{2(3x^2 + p)},$$

$$x_2 = -\frac{x}{2} - \frac{\sqrt{-4p^3 - 27q^2}}{2(3x^2 + p)};$$

d'où il résulte que x_1 et x_2 s'exprimeront en fonction rationnelle de x et des quantités connues, si $\sqrt{-4p^3 - 27q^2}$ est exprimable en fonction rationnelle des quantités connues dont p et q dépendent.

On peut simplifier les précédentes expressions de x_1 et x_2. Nous ferons d'abord

$$(6) \qquad 4p^3 + 27q^2 = -r^2,$$

r pouvant être réel ou imaginaire; et remarquant ensuite que x doit satisfaire à l'équation (1), nous remplacerons dans les valeurs de x_1 et x_2, x^2 par $-\frac{px + q}{x}$, on aura ainsi

$$x_1 = -\frac{x}{2} - \frac{rx}{2(2px + 3q)},$$

$$x_2 = -\frac{x}{2} + \frac{rx}{2(2px + 3q)}.$$

Comme ces deux formules se déduisent l'une de l'autre par le changement de r en $-r$, les valeurs de x_1 et x_2

seront toutes deux comprises dans la formule unique

$$(7)\qquad \left\{\begin{aligned} X &= -\frac{x}{2} + \frac{rx}{2(2px+3q)}, \\ &= \frac{-2px^2 + (r-3q)x}{2(2px+3q)}, \end{aligned}\right.$$

où l'on remplacera r successivement par ses deux valeurs tirées de l'équation (6).

X est une fonction rationnelle non entière d'une racine x de l'équation (1); on pourra donc, par l'un des procédés indiqués dans la troisième leçon, mettre sa valeur sous la forme d'un polynôme du second degré en x.

Pour cela, on divisera d'abord le premier membre de l'équation (1) par $2px + 3q$, et l'on sera conduit ainsi à l'égalité suivante :

$$\begin{aligned} 8p^3(x^3+px+q) = (2px+3q)(4p^2x^2 - 6pqx + 4p^3 + 9q^2) \\ - q(4p^3+27q^2) = 0, \end{aligned}$$

d'où l'on tire

$$2px + 3q = \frac{-qr^2}{4p^2x^2 - 6pqx + 4p^3 + 9q^2},$$

et la valeur de X, donnée par l'équation (7), sera alors

$$\begin{aligned} X &= \frac{-1}{2qr^2}[-2px^2 + (r-3q)x][4p^2x^2 - 6pqx + 4p^3 + 9q^2) \\ &= \frac{1}{2qr^2}\begin{bmatrix} 8p^3x^4 - 4p^2rx^3 + (8p^4 + 6pqr)x^2 \\ -(4p^3+9q^2)(r-3q)x \end{bmatrix}; \end{aligned}$$

enfin on chassera de cette expression de X, x^3 et x^4, à l'aide des équations

$$x^3 = -px - q, \qquad x^4 = -px^2 - qx,$$

et l'on aura

$$(8)\qquad X = \frac{1}{2r}[6px^2 - (9q + r)x + 4p^2].$$

Telle est la formule la plus simple par laquelle on puisse exprimer deux racines de l'équation (1) en fonction rationnelle de la troisième et des quantités connues, lorsque r est une quantité rationnelle.

Mais on peut aussi, comme nous l'avons remarqué dans la troisième leçon, mettre cette valeur de X sous la forme d'une fraction ayant pour numérateur et pour dénominateur un binôme du premier degré en x.

Pour cela, on divisera le premier membre de l'équation (1) par $6px^2-(9q+r)x+4p^2$, après l'avoir préalablement multiplié par $36p^2$ pour éviter les dénominateurs; on trouvera pour quotient

$$6px+(9q+r),$$

et pour reste

$$2r(9q-r)x-4p^2r,$$

en ayant égard à l'équation (6). On aura donc

$$\begin{aligned}&36p^2(x^3+px+q)\\&=[6px^2-(9q+r)x+4p^2][6px+(9q+r)]\\&+[2r(9q-r)x-4p^2r]=0,\end{aligned}$$

et par conséquent

$$6px^2-(9q+r)x+4p^2=\frac{-2r(9q-r)x+4p^2r}{6px+(9q+r)};$$

la valeur de X sera donc

$$\text{(9)}\qquad X=\frac{-(9q-r)x+2p^2}{6px+(9q+r)}.$$

Si p et q désignent des quantités numériques déterminées, et que la quantité $4p^3+27q^2=-r^2$ soit négative, ce qui est la condition nécessaire pour que l'équation (1) ait ses trois racines réelles, les deux valeurs de r seront réelles et de signes contraires; en désignant donc spécialement par r celle de ces deux valeurs qui est posi-

tive, on aura les expressions suivantes des deux racines x_1 et x_2 en fonction de la troisième x,

$$(10)\quad x_1 = \frac{-(9q-r)x+2p^2}{6px+(9q+r)}, \quad x_2 = \frac{-(9q+r)x+2p^2}{6px+(9q-r)}.$$

Nous allons faire, dans ce qui va suivre, une application assez importante de ces formules.

Étude d'une classe étendue d'équations numériques du troisième degré, qui possèdent une propriété remarquable.

Si l'on développe en fraction continue, conformément à la méthode de Lagrange, les trois racines x, x_1, x_2 de l'équation

$$x^3 - 7x + 7 = 0,$$

on trouve

$$-x = 3 + \frac{1}{y}, \quad x_1 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{y}}}},$$

$$x_2 = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{y}}}},$$

y désignant la racine plus grande que 1 de l'équation

$$y^3 - 20y^2 - 9y + 1 = 0,$$

en sorte que les trois fractions continues, dans lesquelles se développent les racines x, x_1, x_2, se terminent par les mêmes quotients.

Cette propriété curieuse de l'équation que nous venons de considérer a été remarquée depuis longtemps, mais

c'est tout récemment que M. Lobatto s'est proposé, le premier, de trouver quelles sont les équations du troisième degré, à coefficients commensurables, qui possèdent cette propriété. Ce géomètre a complétement résolu la question, pour les équations de la forme

$$x^3 + px + q = 0,$$

dans un Mémoire qui fait partie du tome IX du *Journal des Mathématiques pures et appliquées* de M. Liouville. Nous suivrons à peu près la marche qu'il a indiquée.

Si une équation du troisième degré, débarrassée du second terme, a ses trois racines réelles, le coefficient de la première puissance de x est négatif; nous considérerons donc l'équation

$$(1) \qquad x^3 - px + q = 0,$$

et nous supposerons p et q positifs et commensurables (le cas de q négatif se ramènerait à celui de q positif par le simple changement de x en $-x$), en sorte que l'équation (1) aura une racine négative et deux racines positives. Nous désignerons par $-x$ la racine négative, par x_1 et x_2 les deux racines positives, et en faisant

$$(2) \qquad r = +\sqrt{4p^3 - 27q^2},$$

on déduira des formules précédemment établies, par de simples changements de signes,

$$(3) \qquad x_1 = \frac{(9q - r)x + 2p^2}{6px + (9q + r)}, \quad x_2 = \frac{(9q + r)x + 2p^2}{6px + (9q - r)}.$$

Supposons maintenant que les fractions continues qui représentent x et x_1 soient terminées par un même quotient complet y; d'après les propriétés des fractions continues, on aura, pour x et x_1, des valeurs de la forme

suivante :

(4) $$x = \frac{Ny + M}{N'y + M'}, \quad x_1 = \frac{Qy + P}{Q'y + P'},$$

M, N, etc., étant des nombres entiers positifs assujettis à vérifier les équations

(5) $$NM' - MN' = \pm 1, \quad QP' - PQ' = \pm 1.$$

De la première des équations (4) on tire

$$y = \frac{M - M'x}{N'x - N},$$

et, en portant cette valeur de y dans la seconde, il vient

(6) $$x_1 = \frac{Ax + B}{A'x + B'},$$

en faisant, pour abréger,

$$A = PN' - QM', \quad B = QM - PN,$$
$$A' = P'N' - Q'M', \quad B' = Q'M - P'N;$$

d'où l'on déduit aisément

(7) $$AB' - BA' = (NM' - MN')(QP' - PQ') = \pm 1.$$

Les valeurs de x_1, données par les équations (3) et (6), doivent être identiques; car, s'il en est autrement, en égalant ces deux valeurs de x_1, on aura une équation du second ou du premier degré dont les coefficients seront commensurables, ou du moins ne contiendront que le radical r : cette équation, après qu'on y aura changé x en $-x$, aura, avec la proposée (1), une ou deux racines communes, et, dans l'un et l'autre cas, le premier membre de l'équation (1) admettra un diviseur linéaire commensurable ou ne contenant que le radical r. Si ce diviseur linéaire est commensurable, l'équation proposée (1) aura une racine commensurable. Si ce diviseur contient le radical r, et que r soit incommensurable, l'équation proposée (1) aura

une racine de la forme $\alpha + \beta r$, elle admettra donc aussi $\alpha - \beta r$ pour racine, et la troisième racine sera alors commensurable; d'où il suit que si l'équation (1) n'a pas de racine commensurable, comme nous le supposons évidemment dans cette recherche, les deux valeurs de x_1, données par les équations (3) et (6), sont nécessairement identiques : on a donc

$$(8) \qquad \frac{9q - r}{A} = \frac{2p^2}{B} = \frac{6p}{A'} = \frac{9q + r}{B'} = \lambda.$$

On peut déterminer aisément la valeur λ commune à chacun de ces rapports. On tire, en effet, de ces équations (8)

$$\lambda^2(AB' - BA') = -4r^2;$$

et comme $AB' - BA'$ doit être égal à ± 1, il faut qu'ici

$$AB' - BA' = -1, \quad \text{et} \quad \lambda^2 = 4r^2,$$

d'où

$$\lambda = \pm 2r;$$

on peut prendre $\lambda = 2r$, car on ramène à ce cas celui de $\lambda = -2r$, en changeant les signes des quantités A, B, A', B', ce qui est évidemment permis; les équations (8) donneront alors

$$\frac{9q - r}{2r} = A, \quad \frac{2p^2}{2r} = B, \quad \frac{6p}{2r} = A', \quad \frac{9q + r}{2r} = B'.$$

Donc, pour que les deux racines $-x$ et x_1 de l'équation (1) se terminent par les mêmes quotients incomplets, il faut que

$$(9) \qquad \frac{9q - r}{2r}, \quad \frac{2p^2}{2r}, \quad \frac{6p}{2r}, \quad \frac{9q + r}{2r},$$

soient des nombres entiers; ce qui exige, en particulier, que r soit commensurable, puisque p et q le sont par hypothèse.

On serait arrivé exactement aux mêmes conditions si, au lieu de considérer les racines $-x$ et x_1, on avait pris $-x$ et x_2.

Je dis maintenant que les conditions que nous venons de trouver sont suffisantes et que, si les quantités (9) sont des nombres entiers, les trois racines de l'équation (1) développées en fraction continue, se termineront par un même quotient complet.

Posons

$$(10) \qquad \frac{9q-r}{2r} = \text{A}, \quad \frac{2p^2}{2r} = \text{B}, \quad \frac{6p}{2r} = \text{A}', \quad \frac{9q+r}{2r} = \text{B}',$$

les formules (3) deviendront

$$(11) \qquad x_1 = \frac{\text{A}x + \text{B}}{\text{A}'x + \text{B}'}, \quad x_2 = \frac{\text{B}'x + \text{B}}{\text{A}'x + \text{A}};$$

les équations (10) donnent d'ailleurs

$$(12) \qquad \text{AB}' - \text{BA}' = -1,$$

et, par hypothèse, A, B, A', B' sont des nombres entiers.

Cela posé, pour établir la proposition que nous avons en vue, nous commencerons par démontrer le lemme suivant :

Lemme. — *Si* A, B, A', B' *sont quatre nombres entiers tels, que* A > B, A' > B', *et qui satisfont à la condition*

$$\text{AB}' - \text{BA}' = \pm 1,$$

on pourra toujours considérer les fractions $\frac{\text{B}}{\text{B}'}$ *et* $\frac{\text{A}}{\text{A}'}$ *comme deux réduites consécutives d'une même fraction continue.*

Réduisons, en effet, $\frac{\text{A}}{\text{A}'}$ en fraction continue, et arrangeons-nous de manière que le nombre des quotients soit pair ou impair, suivant que AB' — BA' est égal à $+1$ ou à -1. Cela est toujours possible; car on peut, si on le

juge à propos, diminuer d'une unité le dernier quotient obtenu, et prendre un quotient de plus égal à 1. Formons les réduites de cette fraction continue, et désignons par $\frac{M}{M'}$ l'avant-dernière, c'est-à-dire celle qui précède $\frac{A}{A'}$, on aura

$$AM' - MA' = \pm 1 = AB' - BA',$$

et, par conséquent,

$$A(M' - B') = A'(M - B).$$

Or, je dis que cette dernière égalité exige que l'on ait $M = B$, $M' = B'$; car si cela n'avait pas lieu, A, qui divise le premier membre de l'égalité précédente, diviserait aussi le second, et comme il est évidemment premier avec A', il diviserait $M - B$, ce qui est impossible, puisque M et B sont tous deux moindres que A.

Il suit de là que l'on peut considérer $\frac{B}{B'}$ comme l'avant-dernière réduite de la fraction continue dans laquelle se développe $\frac{A}{A'}$. Notre lemme est donc démontré.

Revenons maintenant au théorème qu'il s'agit d'établir (*).

Si l'on a à la fois

$$A > B, \quad A' > B', \quad x > 1,$$

il est évident, d'après la première équation (11), que x sera un quotient complet de la fraction continue dans laquelle se développe x_1; car, à cause de l'équation (12), si l'on fait le développement de $\frac{A}{A'}$ en fraction continue, on

(*) Le Mémoire de M. Lobatto renferme quelques inexactitudes, qui pourtant n'infirment en rien les conclusions de l'auteur.

aura, par exemple,

$$\frac{A}{A'} = \alpha + \cfrac{1}{\beta + \ddots + \cfrac{1}{\gamma + \cfrac{1}{\delta}}}, \qquad \frac{B}{B'} = \alpha + \cfrac{1}{\beta + \ddots + \cfrac{1}{\gamma}},$$

et, d'après les propriétés des fractions continues,

$$x_1 = \alpha + \cfrac{1}{\beta + \ddots + \cfrac{1}{\gamma + \cfrac{1}{\delta + \cfrac{1}{x}}}}.$$

Supposons que l'on n'ait pas à la fois $A > B$, $A' > B'$, mais que x soit > 1, et posons

$$x = a + \frac{1}{z},$$

a étant le plus grand entier contenu dans x, la valeur de x_1 devient

$$x_1 = \frac{(Aa + B)z + A}{(A'a + B')z + A'} = \frac{Cz + A}{C'z + A'};$$

ici l'on a évidemment, a n'étant pas nul,

$$C > A, \quad C' > A'$$

et

$$CA' - AC' = +1, \quad \text{à cause de} \quad AB' - BA' = -1;$$

d'où il résulte, évidemment, que z sera un quotient complet de la fraction continue dans laquelle x_1 se développe. Cette conclusion est en défaut si a est nul; car alors la valeur de x_1 est

$$x_1 = \frac{Bz + A}{B'z + A'},$$

et il se peut qu'on n'ait pas à la fois $B > A$ et $B' > A'$. Posons alors

$$z = b + \frac{1}{u},$$

b étant l'entier le plus grand contenu dans z; on aura

$$x_1 = \frac{(Bb + A)u + B}{(B'b + A')u + B'} = \frac{Du + B}{D'u + B'}.$$

Comme b ne peut être nul, on a évidemment $D > B$, $D' > B'$; d'ailleurs $DB' - BD' = -1$, donc u sera un quotient complet de x_1.

Il résulte de ce qui précède que l'un des trois premiers quotients complets de la racine négative $-x$ sera nécessairement un quotient complet de la racine positive x_1, et par conséquent aussi de la racine x_2; car tous nos raisonnements s'appliquent à x_2 qui se déduit de x_1, en changeant A et B' l'un dans l'autre.

Formation des équations qui possèdent la propriété précédente. — Nous allons former les équations qui possèdent la propriété que nous venons d'étudier.

Il s'agit des équations de la forme

$$x^3 - px + q = 0,$$

et qui sont telles, qu'en posant

$$r^2 = 4p^3 - 27q^2,$$

on ait

(1) $$9q - r = 2rA,$$

(2) $$p^2 = rB,$$

(3) $$3p = rA',$$

(4) $$(9q + r) = 2rB',$$

A, B, A', B' étant des nombres entiers; et il en résulte

(5) $$AB' - BA' = -1.$$

L'équation (5) étant une conséquence des quatre premières, nous pouvons nous borner aux équations (1), (3), (4), (5), et même substituer aux équations (1) et (4) celles qu'on en déduit par addition et soustraction, savoir :

$$9q = r(A + B'), \quad B' - A = 1.$$

De ces dernières combinées avec les équations (3) et (5), on tire

$$(6) \qquad B' = A + 1,$$

$$(7) \qquad B = \frac{A^2 + A + 1}{A'},$$

$$(8) \qquad q = \frac{2A + 1}{9} r,$$

$$(9) \qquad p = \frac{A'}{3} r.$$

Des équations (8) et (9), combinées avec l'équation $r^2 = 4p^3 - 27q^2$, on tire

$$r = \frac{9(2A+1)^2 + 27}{4A'^3};$$

par suite, les équations (8) et (9) donnent

$$p = 3\frac{(2A+1)^2 + 3}{4A'^2} = \frac{3(A^2 + A + 1)}{A'^2},$$

$$q = \frac{(2A+1)^3 + 3(2A+1)}{4A'^3} = \frac{2A^3 + 3A^2 + 3A + 1}{A'^3}.$$

Dans ces formules, A peut être considéré comme un nombre entier absolument arbitraire, et A' n'est assujetti qu'à la seule condition de satisfaire à l'équation (7), c'est-à-dire de diviser $A^2 + A + 1$.

Il résulte de là que les équations du troisième degré

dont nous nous occupons ont la forme générale que voici :

$$x^3 - 3\frac{A^2+A+1}{A'^2}x + \frac{2A^3+3A^2+3A+1}{A'^3} = 0,$$

A désignant un nombre entier quelconque, et A′ un diviseur quelconque de A^2+A+1. L'équation $x^3-7x+7=0$ se déduit de cette équation générale, en faisant $A=4$, $A'=3$.

M. Lobatto s'est borné, dans son Mémoire, à l'étude des équations du troisième degré débarrassées du second terme. On arriverait à des résultats plus étendus, en considérant les équations complètes; car on comprend qu'une équation complète puisse posséder la propriété que M. Lobatto a étudiée, et ne pas la conserver quand on l'aura débarrassée de son second terme. Cette extension des recherches de M. Lobatto ne présente aucune difficulté, car l'équation la plus générale du troisième degré peut être mise sous la forme

$$(x-a)^3 + p(x-a) + q = 0,$$

et l'on peut aisément exprimer deux racines en fonction rationnelle de la troisième, en se servant des formules que nous avons établies précédemment. Ces formules feront connaître ensuite les conditions, pour que les fractions continues dans lesquelles se développent les trois racines puissent se terminer par les mêmes quotients incomplets : il n'y a qu'à employer des raisonnements tout semblables à ceux que nous avons faits; mais je crois devoir me borner ici à cette simple indication. Au surplus, on trouvera dans la Note VII l'extension la plus complète qu'on puisse désirer des résultats que nous avons exposés dans cette leçon.

DIX-SEPTIÈME LEÇON.

Résolution de l'équation générale du quatrième degré. — Méthode de Louis Ferrari. — Étude de la resolvante. — Méthode de Lagrange. — Méthode de Descartes. — Méthode de Tschirnaüs et d'Euler.

Résolution de l'équation générale du quatrième degré.

Nous allons examiner, dans cette leçon, les principales méthodes connues pour la résolution de l'équation générale du quatrième degré.

Méthode de Louis Ferrari.

La méthode la plus simple pour résoudre l'équation du quatrième degré, est aussi la plus ancienne; c'est celle de Louis Ferrari : elle consiste à faire en sorte que les deux membres de l'équation soient des carrés, et elle ramène par suite la résolution de l'équation du quatrième degré à celle de deux équations du second.

Soit l'équation

$$(1) \qquad x^4 + px^3 + qx^2 + rx + s = 0;$$

en ne conservant dans le premier membre que les deux premiers termes, elle devient

$$x^4 + px^3 = -qx^2 - rx - s,$$

et, en ajoutant aux deux membres $\frac{p^2x^2}{4}$, afin que le premier membre devienne un carré,

$$(2) \qquad \left(x^2 + \frac{p}{2}x\right)^2 = \left(\frac{p^2}{4} - q\right)x^2 - rx - s.$$

Mise sous cette forme, l'équation proposée se résoudrait immédiatement, si le second membre était un carré; car il suffirait alors d'extraire la racine carrée des deux membres, et l'équation ne serait plus que du second degré.

C'est à ce cas très-particulier que la méthode de Ferrari ramène tous les autres.

Désignons par y une quantité indéterminée, et ajoutons aux deux membres de l'équation (2) la même quantité

$$\left(x^2 + \frac{p}{2}x\right)y + \frac{y^2}{4},$$

il vient

$$(3)\quad \left(x^2 + \frac{p}{2}x + \frac{y}{2}\right)^2 = \left(\frac{p^2}{4} - q + y\right)x^2 + \left(\frac{py}{2} - r\right)x + \left(\frac{y^2}{4} - s\right).$$

Maintenant, déterminons y, de manière que le second membre de l'équation (3) soit un carré. Il suffit, pour cela, que l'on ait

$$\left(\frac{py}{2} - r\right)^2 = \left(\frac{p^2}{4} - q + y\right)(y^2 - 4s),$$

ou

$$(4)\quad y^3 - qy^2 + (pr - 4s)y - s(p^2 - 4q) - r^2 = 0;$$

et, si l'on connaît une seule racine de cette équation en y, la résolution de l'équation proposée (1) s'ensuivra immédiatement, car l'équation (3), qui est la même que (1), peut s'écrire comme il suit :

$$\left(x^2 + \frac{p}{2}x + \frac{y}{2}\right)^2 - \left(\frac{p^2}{4} - q + y\right)\left[x + \frac{p\frac{y}{2} - r}{2\left(\frac{p^2}{4} - q + y\right)}\right]^2 = 0,$$

et elle se décompose dans les deux suivantes, qui sont du second degré :

$$(5)\quad \left\{\begin{aligned} &x^2 + \left(\frac{p}{2} + \sqrt{\frac{p^2}{4} - q + y}\right)x + \left[\frac{y}{2} + \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}}\right] = 0, \\ &x^2 + \left(\frac{p}{2} - \sqrt{\frac{p^2}{4} - q - y}\right)x + \left[\frac{y}{2} - \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}}\right] = 0. \end{aligned}\right.$$

L'équation (4), qui est du troisième degré, sera donc ici la *réduite* ou la *résolvante* de l'équation (1). Nous avons vu qu'on peut exprimer par radicaux les racines de l'équation générale du troisième degré; il s'ensuit que l'équation du quatrième degré jouit de la même propriété, car les équations (5) permettent d'exprimer les quatre racines de l'équation (1) en fonction des coefficients et d'une racine quelconque y de la résolvante.

EXEMPLE. — Considérons l'équation

$$x^4 + x^3 - 4x^2 - 4x + 1 = 0,$$

dont les racines ont pour valeurs absolues le côté et les diagonales du polygone régulier de trente côtés inscrit dans le cercle de rayon 1. La résolvante (4) est ici

$$y^3 + 4y^2 - 8y - 33 = 0,$$

et elle a — 3 pour racine; l'équation proposée se décompose alors dans les deux suivantes :

$$x^2 + \frac{1+\sqrt{5}}{2}x - \left(\frac{-1+\sqrt{5}}{2}\right)^2 = 0,$$

$$x^2 + \frac{-1+\sqrt{5}}{2}x - \left(\frac{1+\sqrt{5}}{2}\right)^2 = 0;$$

et, en général, en appliquant la méthode de Ferrari à une équation du quatrième degré à coefficients commensurables dont les racines ne doivent pas contenir, dans leur expression, de radicaux cubiques, on arrivera toujours à une résolvante qui aura une racine commensurable.

Étude de la résolvante.

Nous venons de voir comment les quatre racines de l'équation proposée peuvent s'exprimer à l'aide d'une seule racine de la résolvante : nous allons étudier à son tour

cette résolvante, et examiner de quelle manière ses racines sont formées avec celles de la proposée.

Désignons toujours par y une racine quelconque de la résolvante, et par x_1, x_2, x_3, x_4 les quatre racines de l'équation proposée, savoir, par x_1 et x_2 celles qui appartiennent à la première des équations (5); par x_3 et x_4 celles qui appartiennent à la seconde. On aura alors

$$x_1 x_2 = \frac{y}{2} + \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}},$$

$$x_3 x_4 = \frac{y}{2} - \frac{\frac{py}{2} - r}{2\sqrt{\frac{p^2}{4} - q + y}};$$

et, en ajoutant,

$$y = x_1 x_2 + x_3 x_4.$$

La résolvante a donc pour racine la fonction

$$x_1 x_2 + x_3 x_4$$

des quatre racines de la proposée, fonction qui n'a effectivement que trois valeurs, quand on y échange les racines les unes dans les autres de toutes les manières possibles.

Posons

$$t = 2\sqrt{\frac{p^2}{4} - q + y},$$

d'où

$$y = \frac{t^2}{4} - \left(\frac{p^2}{4} - q\right);$$

la résolvante en y se transformera dans une équation en t, qui sera du sixième degré, mais qui ne contiendra que des puissances paires de t. Cette équation ne sera pas plus difficile à résoudre que l'équation (4), et on peut la prendre pour résolvante à la place de cette dernière. Les

équations (5), dans lesquelles se décompose l'équation proposée, deviennent alors

$$x^2+\left(\frac{p+t}{2}\right)x+\frac{1}{2}\left(\frac{t^2}{4}-\frac{p^2}{4}+q\right)+\frac{\frac{p}{2}\left(\frac{t^2}{4}-\frac{p^2}{4}+q\right)-r}{2t}=0,$$

$$x^2+\left(\frac{p-t}{2}\right)x+\frac{1}{2}\left(\frac{t^2}{4}-\frac{p^2}{4}+q\right)-\frac{\frac{p}{2}\left(\frac{t^2}{4}-\frac{p^2}{4}+q\right)-r}{2t}=0,$$

et l'on en déduira les quatre racines de la proposée, si l'on connait une seule racine de la résolvante en t.

Les équations précédentes ont pour racines, la première, x_1 et x_2, la seconde, x_3 et x_4; on a donc

$$x_1+x_2=\frac{p+t}{2},$$

$$x_3+x_4=\frac{p-t}{2},$$

et, en retranchant,

$$t=x_1+x_2-x_3-x_4.$$

Telle est l'expression de la racine de la résolvante en t. C'est une fonction linéaire des racines de la proposée, qui peut prendre effectivement six valeurs égales deux à deux et de signes contraires, par les permutations des racines x_1, x_2, x_3, x_4.

Méthode de Lagrange.

D'après la théorie générale exposée dans les onzième et douzième leçons, on peut exprimer rationnellement les quatre racines de l'équation générale du quatrième degré par une fonction de ces racines telle, que les $1.2.3.4$ valeurs qu'on en déduit par les permutations soient différentes. Une pareille fonction dépend d'une équation du vingt-quatrième degré; mais nous venons de voir, par

l'analyse de la méthode de Ferrari, qu'il suffit, pour résoudre l'équation du quatrième degré, de connaître une fonction des racines qui ait trois valeurs seulement, ou six valeurs égales deux à deux et de signes contraires.

La formation à priori de l'équation dont dépend une pareille fonction des racines de la proposée, et la détermination subséquente de ses racines, constituent une nouvelle méthode due à Lagrange, et que nous allons actuellement exposer.

Soit l'équation

(1) $$x^4 + px^3 + qx^2 + rx + s = 0,$$

et désignons par x_1, x_2, x_3, x_4 ses quatre racines. La fonction la plus simple de ces racines, parmi celles qui ne peuvent acquérir que trois valeurs, est $x_1 x_2 + x_3 x_4$; posons donc

$$y = x_1 x_2 + x_3 x_4$$

et commençons par chercher la valeur de y, ou plutôt l'équation du troisième degré dont elle dépend.

Soient y_1, y_2, y_3 les trois valeurs que peut acquérir y, on aura

$$y_1 = x_1x_2 + x_3x_4, \quad y_2 = x_1x_3 + x_2x_4, \quad y_3 = x_1x_4 + x_2x_3,$$

et l'équation en y sera

(2) $$y^3 - (y_1+y_2+y_3)y^2 + (y_1y_2+y_1y_3+y_2y_3)y - y_1y_2y_3 = 0.$$

Les coefficients de cette équation (2) sont des fonctions symétriques des racines de l'équation (1), et peuvent, par conséquent, s'exprimer par les coefficients p, q, r, s. On a

$$y_1 + y_2 + y_3 = (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) = q,$$

$$\begin{aligned} &y_1y_2 + y_1y_3 + y_2y_3 \\ &= (x_1 + x_2 + x_3 + x_4)(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) \\ &\quad - 4x_1x_2x_3x_4 = pr - 4s, \end{aligned}$$

$$\begin{aligned} &y_1y_2y_3 = x_1x_2x_3x_4 \\ &\times[(x_1+x_2+x_3+x_4)^2 - 4(x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4)] \\ &+ (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)^2 = s(p^2 - 4q) + r^2; \end{aligned}$$

l'équation résolvante en y est donc

$$(3)\quad y^3 - qy^2 + (pr - 4s)y - [s(p^2 - 4q) + r^2] = 0.$$

Nous savons résoudre cette équation, qui est du troisième degré ; voyons maintenant comment on obtiendra les valeurs des racines x_1, x_2, x_3, x_4.

Soit y_1 une racine quelconque de l'équation (3), on aura

$$x_1 x_2 + x_3 x_4 = y_1 ;$$

d'ailleurs

$$x_1 x_2 \times x_3 x_4 = s ;$$

donc $x_1 x_2$ et $x_3 x_4$ sont les racines de l'équation du second degré

$$(4)\quad z^2 - y_1 z + s = 0.$$

Soient z_1 et z_2 les racines de cette équation (4), on aura

$$x_1 x_2 = z_1, \quad x_3 x_4 = z_2 ;$$

connaissant ainsi les fonctions $x_1 x_2$ et $x_3 x_4$, on voit de suite qu'on doit en déduire rationnellement les sommes $x_1 + x_2$ et $x_3 + x_4$, qui sont des fonctions respectivement semblables à $x_1 x_2$ et $x_3 x_4$. On a, effectivement,

$$x_3 x_4 (x_1 + x_2) + x_1 x_2 (x_3 + x_4) = -r,$$

ou

$$z_2 (x_1 + x_2) + z_1 (x_3 + x_4) = -r ;$$

d'ailleurs

$$(x_1 + x_2) + (x_3 + x_4) = -p,$$

donc

$$x_1 + x_2 = \frac{r - pz_2}{z_2 - z_1}, \quad x_3 + x_4 = \frac{pz_1 - r}{z_2 - z_1}.$$

Connaissant $x_1 + x_2$ et $x_1 x_2$, $x_3 + x_4$ et $x_3 x_4$, on peut former deux équations du second degré, ayant pour racines, la première, x_1 et x_2, la seconde, x_3 et x_4, et le problème peut être considéré comme résolu.

On résout plus facilement l'équation du quatrième degré, en prenant une résolvante dont la racine soit une fonction linéaire des racines de l'équation proposée, ayant six valeurs égales deux à deux et de signes contraires.

Soit

$$t = x_1 + x_2 - x_3 - x_4;$$

cette fonction, ayant six valeurs, dépendra d'une équation du sixième degré : mais parce que ces valeurs de t sont égales deux à deux et de signes contraires, l'équation s'abaissera au troisième degré, en posant

$$t^2 = \theta.$$

On peut former directement l'équation en θ, puisqu'on connaît la composition de ses racines; mais on peut aussi la déduire de la résolvante (3) en y. Il est facile, en effet, de voir que l'on a

$$y = \frac{\theta - p^2 + 4q}{4},$$

et la résolvante en θ est

$$(5) \left\{ \begin{array}{l} \theta^3 - (3p^2 - 8q)\theta^2 + (3p^4 - 16p^2q + 16q^2 + 16pr - 64s)\theta \\ \quad - (p^3 - 4pq + 8r)^2 = 0. \end{array} \right.$$

On pourrait exprimer les quatre racines x_1, x_2, x_3, x_4 de la proposée, à l'aide d'une seule des racines θ de cette équation; mais on obtient des résultats plus simples en employant les trois racines.

Soient θ_1, θ_2, θ_3 les trois racines de l'équation (5), on aura

$$(6) \quad \left\{ \begin{array}{l} x_1 + x_2 - x_3 - x_4 = \sqrt{\theta_1}, \\ x_1 + x_3 - x_2 - x_4 = \sqrt{\theta_2}, \\ x_1 + x_4 - x_2 - x_3 = \sqrt{\theta_3}; \end{array} \right.$$

d'ailleurs

$$(7) \quad x_1 + x_2 + x_3 + x_4 = -p,$$

et les équations (6) et (7), qui sont du premier degré, donneront les valeurs suivantes des quatre racines :

$$x_1 = \frac{-p + \sqrt{\theta_1} + \sqrt{\theta_2} + \sqrt{\theta_3}}{4},$$

$$x_2 = \frac{-p + \sqrt{\theta_1} - \sqrt{\theta_2} - \sqrt{\theta_3}}{4},$$

$$x_3 = \frac{-p - \sqrt{\theta_1} + \sqrt{\theta_2} - \sqrt{\theta_3}}{4},$$

$$x_4 = \frac{-p - \sqrt{\theta_1} - \sqrt{\theta_2} + \sqrt{\theta_3}}{4}.$$

Ces quatre racines peuvent être représentées par la formule unique

(8) $$x = \frac{-p + \sqrt{\theta_1} + \sqrt{\theta_2} + \sqrt{\theta_3}}{4},$$

puisque chaque radical a deux valeurs égales et de signes contraires. Mais ici se présente une difficulté, car l'expression de x, donnée par la formule (8), a huit valeurs, tandis que l'équation proposée ne peut avoir que quatre racines. Il est aisé de faire disparaître cette ambiguïté. En effet, on peut prendre à volonté l'une des deux valeurs de $\sqrt{\theta_1}$ et de $\sqrt{\theta_2}$; mais quand on a fixé ces valeurs, celle du troisième radical $\sqrt{\theta_3}$ se trouve par cela même déterminée. En effet, en multipliant les trois équations (6), on trouve

$$\begin{aligned}\sqrt{\theta_1}\ \sqrt{\theta_2}\ \sqrt{\theta_3} = {} & (x_1^3 + x_2^3 + x_3^3 + x_4^3) \\ & + 2\,(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) \\ & - x_1\,(x_2^2 + x_3^2 + x_4^2) - x_2\,(x_1^2 + x_3^2 + x_4^2) \\ & - x_3\,(x_1^2 + x_2^2 + x_4^2) - x_4\,(x_1^2 + x_2^2 + x_3^2) \\ = {} & 2\sum x_1^3 + 2\sum x_1x_2x_3 - \sum x_1 \sum x_1^2 \\ = {} & -p^3 + 4pq - 8r,\end{aligned}$$

d'où

$$\sqrt{\theta_3} = \frac{-p^3 + 4pq - 8r}{\sqrt{\theta_1}\sqrt{\theta_2}}.$$

Il résulte de là que la valeur de x, donnée par l'équation (8), a précisément quatre valeurs, et qu'elle représente bien, en conséquence, les quatre racines de l'équation proposée.

Remarque. — Il est important de remarquer que le succès des méthodes de Ferrari et de Lagrange est dû à cette seule circonstance, *que l'on peut former des fonctions de quatre lettres, qui n'ont que trois valeurs.*

Méthode de Descartes.

Cette méthode consiste à identifier l'équation proposée

$$x^4 + px^3 + qx^2 + rx + s = 0,$$

avec cette autre

$$(x^2 + fx + g)(x^2 + f'x + g') = 0,$$

dont les racines peuvent être considérées comme connues.

Au lieu d'employer la méthode des coefficients indéterminés, comme fait Descartes, on peut exprimer que $x^2 + fx + g$ est un diviseur du premier membre de l'équation proposée, en effectuant la division, et égalant à zéro les deux termes du reste qui est du premier degré en x. On obtient ainsi deux équations entre les deux inconnues f et g, et en éliminant g ou f, on a une équation du sixième degré qu'on ramène aisément au troisième, et qu'on peut considérer comme une résolvante de l'équation proposée. Cette méthode ne diffère pas, au fond, de celles que nous avons d'abord exposées; car si l'on connaît une valeur de g ou de f, c'est-à-dire $x_1 x_2$ ou $x_1 + x_2$, on connaîtra également $x_3 x_4$ ou $x_3 + x_4$, et la résolu-

tion de l'équation proposée s'en déduira comme nous l'avons montré précédemment.

Méthodes de Tschirnaüs et d'Euler.

Je n'ajouterai rien à ce que j'ai dit dans une précédente leçon au sujet de la méthode de Tschirnaüs, qui ramène l'équation

$$x^4 + px^3 + qx^2 + rx + s = 0$$

à la forme bicarrée, en employant la transformation

$$y = a + bx + x^2,$$

et disposant convenablement des indéterminées a et b.

La méthode d'Euler consiste à éliminer y entre les deux équations

$$x = a + by + cy^2 + dy^3,$$
$$y^4 = e,$$

et à identifier l'équation finale en x avec la proposée dont les racines seront alors données par la formule

$$x = a + b\sqrt[4]{e} + c(\sqrt[4]{e})^2 + d(\sqrt[4]{e})^3.$$

Tout revient donc à déterminer les valeurs des indéterminées a, b, c, d, e, dont l'une peut être choisie arbitrairement.

DIX-HUITIÈME LEÇON.

Sur la résolution algébrique des équations. — Des équations de degré premier. — Des équations de degré non premier.

Sur la résolution algébrique des équations.

Toutes les méthodes connues que les géomètres ont essayé d'appliquer à la résolution algébrique des équations, et il en serait nécessairement de même des nouvelles qu'on pourrait imaginer, reviennent à faire dépendre la résolution de l'équation proposée de celle d'une autre équation plus facile à résoudre, et dont les racines sont des fonctions de celles de la proposée.

C'est ainsi que nous avons pu résoudre l'équation du troisième degré, en déterminant la valeur d'une fonction linéaire des racines x_1, x_2, x_3, savoir :

$$t = x_1 + \alpha x_2 + \alpha^2 x_3,$$

α désignant l'une des racines imaginaires de l'équation $x^3 = 1$. Le cube t^3 de cette fonction ne peut prendre que deux valeurs distinctes par les permutations des racines x_1, x_2, x_3, et dépend, par conséquent, d'une équation du second degré.

De même, nous avons résolu l'équation du quatrième degré en déterminant la valeur de l'une des deux fonctions suivantes de ses racines x_1, x_2, x_3, x_4,

$$y = x_1 x_2 + x_3 x_4,$$
$$t = x_1 - x_2 + x_3 - x_4.$$

La première de ces deux fonctions ne peut acquérir que trois valeurs, et dépend, par conséquent, d'une équation

du troisième degré, qu'on sait résoudre; la seconde peut prendre six valeurs et dépend d'une équation du sixième degré, mais qu'on peut abaisser au troisième, parce qu'elle ne contient que des puissances paires de l'inconnue. Nous avons vu, dans la leçon précédente, que la résolvante en t conduit plus aisément que celle en y à la résolution de la proposée; elle a aussi cet avantage, que la résolution de l'équation du quatrième degré, qu'on en déduit, présente la plus complète analogie avec celle de l'équation du troisième degré. La fonction t peut, en effet, s'écrire ainsi :

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4,$$

α désignant la racine réelle -1 de l'équation $x^4 = 1$.

Dans les *Mémoires de l'Académie de Berlin* (années 1770 et 1771) (*), Lagrange, prenant pour point de départ les résultats qui précèdent, a cherché à opérer la résolution de l'équation de degré m dont $x_1, x_2, x_3, \ldots, x_m$ sont les m racines, en employant une fonction de la forme

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-2} x_{m-1} + \alpha^{m-1} x_m,$$

où α désigne une racine de l'équation $x^m = 1$.

Quoique ces recherches de Lagrange ne l'aient pas conduit à la résolution des équations générales d'un degré supérieur au quatrième, les développements qu'il a donnés à ce sujet présentent assez d'intérêt pour qu'il semble utile de les exposer ici.

Nous suivrons la marche tracée par l'illustre auteur, et nous distinguerons avec lui le cas où le degré de l'équation est un nombre premier, et le cas où ce degré est un nombre composé.

(*) Lagrange a donné un extrait de son Mémoire dans la Note XIII de son *Traité de la Résolution des équations numériques*, 3e édition, page 242.



Des équations de degré premier.

Soient

$$x_1,\ x_2,\ x_3,\ldots,\ x_m$$

les m racines d'une équation

(1) $$V = 0,$$

d'un degré premier m, α une racine quelconque de l'équation $x^m = 1$, et posons

(2) $$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m.$$

Si α n'est pas égal à 1, m étant premier, les puissances de α, savoir

$$1,\ \alpha,\ \alpha^2,\ldots,\ \alpha^{m-1},$$

sont les m racines de l'équation $x^m = 1$, et, par conséquent, sont toutes distinctes. Il résulte de là que la fonction t prendra $1.2.3\ldots m$ valeurs distinctes, si l'on y permute les m racines x_1, x_2, etc.; cette fonction dépend donc d'une équation du degré

$$1.2.3\ldots m,$$

qu'on peut former par la méthode exposée dans la troisième leçon, puisqu'on connaît la composition de ses racines.

Nous allons démontrer que *la résolution de cette équation de degré $1.2.3\ldots m$ peut se ramener à la résolution d'une équation du degré $m-1$, dont les coefficients dépendent d'une équation du degré $1.2.3\ldots(m-2)$.*

Multiplions successivement l'expression de t par α, α^2, $\alpha^3,\ldots,\alpha^{m-1}$, et rabaissons les exposants de α au-dessous de m, à l'aide de la relation $\alpha^{m+n} = \alpha^n$; on aura

$$\begin{aligned}
t &= x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m,\\
\alpha t &= \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3 + \ldots + x_m,\\
\alpha^2 t &= \alpha^2 x_1 + \alpha^3 x_2 + \alpha^4 x_3 + \ldots + \alpha x_m,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\alpha^{m-1} t &= \alpha^{m-1} x_1 + x_2 + \alpha x_3 + \ldots + \alpha^{m-2} x_m,
\end{aligned}$$

ou, en ordonnant par rapport aux puissances de α,

$$(3)\quad \left\{\begin{array}{l} t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m, \\ \alpha t = x_m + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{m-1} x_{m-1}, \\ \alpha^2 t = x_{m-1} + \alpha x_m + \alpha^2 x_1 + \ldots + \alpha^{m-1} x_{m-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha^{m-1} t = x_2 + \alpha x_3 + \alpha^2 x_4 + \ldots + \alpha^{m-1} x_1. \end{array}\right.$$

On voit que chacune des quantités

$$t,\ \alpha t,\ \alpha^2 t, \ldots,\ \alpha^{m-1} t$$

se déduit de la précédente par la substitution

$$\begin{pmatrix} x_1, & x_2, & \ldots, & x_m \\ x_m, & x_1, & \ldots, & x_{m-1} \end{pmatrix},$$

et, par conséquent, chacune des racines x_1, x_2, etc., occupe, dans les seconds membres des équations (3), toutes les places. Par exemple, x_1 est à la première place dans t, à la deuxième dans αt, etc., à la dernière place dans $\alpha^{m-1} t$; on aura donc les $1.2.3\ldots m$ valeurs de t, en faisant subir aux $m-1$ lettres $x_2, x_3, \ldots, x_m$, dans les seconds membres des équations (3), les $1.2.3\ldots(m-1)$ permutations dont elles sont susceptibles, sans changer la place de x_1. Et si l'on fait, pour abréger,

$$\mu = 1.2.3\ldots(m-1),$$

et que l'on désigne par

$$t_1,\ t_2,\ t_3, \ldots,\ t_\mu$$

les μ valeurs que prend t, quand on y permute les $m-1$ lettres $x_2, x_3, \ldots, x_m$, les $1.2.3\ldots m$ racines de l'équa-

tion en t seront

$$\begin{array}{l} t_1,\ \alpha t_1,\ \alpha^2 t_1,\ldots,\ \alpha^{m-1} t_1,\\ t_2,\ \alpha t_2,\ \alpha^2 t_2,\ldots,\ \alpha^{m-1} t_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ t_\mu,\ \alpha t_\mu,\ \alpha^2 t_\mu,\ldots,\ \alpha^{m-1} t_\mu; \end{array}$$

on a d'ailleurs

$$(t-t_p)\ (t-\alpha t_p)\ldots(t-\alpha^{m-1}t_p) = t^m - t_p^m,$$

l'équation en t sera donc

$$\left(t^m - t_1^m\right)\ \left(t^m - t_2^m\right)\cdots\left(t^m - t_\mu^m\right) = 0.$$

On voit que cette équation ne contient que des puissances de t dont les exposants sont divisibles par m, et qu'elle s'abaissera au degré $\mu = 1.2.3\ldots(m-1)$, en posant

$$t^m = \theta.$$

L'expression de θ est

(4) $$\theta = (x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m)^m,$$

et l'on déduit de cette formule les μ racines de l'équation en θ, en permutant, de toutes les manières possibles, les $m-1$ lettres $x_2, x_3,\ldots, x_m$, sans changer x_1 de place. Or, parmi ces permutations, qui servent à déduire toutes les valeurs de θ de l'une d'entre elles, il en est qui méritent surtout de fixer l'attention, parce qu'elles équivalent au simple changement de α en $\alpha^2, \alpha^3,\ldots, \alpha^{m-1}$. En effet, m étant un nombre premier, si dans la série

$$\alpha,\ \alpha^2,\ldots,\ \alpha^{m-1}$$

on remplace α par α^n, n étant $< m$, on reproduira les mêmes racines, mais dans un ordre différent. La substitution à α, de l'une de ses puissances, équivaut donc à

un certain changement des puissances de α entre elles dans l'expression de θ, et, par suite, à un certain changement des racines $x_2, x_3, \ldots, x_m$ entre elles.

Remplaçons donc α, dans l'expression (4) de θ, par chacune de ses puissances $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{m-1}$, rabaissons les exposants de α au-dessous de m et ordonnons, par rapport aux puissances de α, la fonction dont la puissance m est égale à θ; désignons enfin par

$$\theta_1,\ \theta_2,\ \theta_3, \ldots,\ \theta_{m-1},$$

les $m-1$ valeurs de θ ainsi obtenues : il est évident que x_2, qui occupe la deuxième place dans θ_1, aura la troisième dans θ_2, la quatrième dans θ_3, etc., la dernière dans θ_{m-1}, et l'on aura

$$(5)\quad \left\{\begin{array}{l} \theta_1 = (x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots\ldots \alpha{+}^{m-1} x_m)^m, \\ \theta_2 = (x_1 + \ldots + \alpha^2 x_2 + \ldots\ldots\ldots\ldots)^m, \\ \theta_3 = (x_1 + \ldots\ldots\ldots + \alpha^3 x_2 + \ldots\ \ldots)^m, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \theta_{m-1} = (x_1 + \ldots\ldots\ldots\ldots\ldots\ldots + \alpha^{m-1} x_2)^m. \end{array}\right.$$

Voilà donc $m-1$ valeurs de θ dans lesquelles x_2 occupe successivement la seconde, la troisième, etc., la dernière place, en sorte qu'il suffira, pour avoir les $1.2.3\ldots(m-1)$ valeurs de θ, de faire, dans chacune des $m-1$ valeurs que nous venons d'écrire les $1.2.3\ldots(m-2)$ permutations des lettres $x_3, x_4, \ldots, x_m$, les unes dans les autres, sans changer la place ni de x_1 ni de x_2. On déduira, en effet, par ce moyen $1.2.3\ldots(m-2)$ valeurs de θ, de chacune des valeurs (5), ce qui fera en tout $1.2.3\ldots(m-1)$ valeurs.

Si maintenant on considère l'équation de degré $m-1$

$$(\theta-\theta_1)\ (\theta-\theta_2)\ldots\ (\theta-\theta_{m-1}) = 0,$$

ou

$$(6) \qquad \theta^{m-1} + P_1 \theta^{m-2} + P_2 \theta^{m-3} + \ldots + P_{m-2}\theta + P_{m-1} = 0,$$

qui a pour racines les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$, je dis que les coefficients P_1, P_2, etc., de cette équation ne dépendent que d'une équation du degré $1.2.3\ldots(m-2)$, en sorte que l'équation du degré $1.2.3\ldots(m-1)$, qui a pour racines toutes les valeurs de θ, se décomposera en $1.2.3\ldots(m-2)$ facteurs du degré $m-1$, à l'aide d'une seule équation du degré $1.2.3\ldots(m-2)$.

D'abord il est facile de voir que toute fonction symétrique des quantités $\theta_1, \theta_2, \theta_3, \ldots, \theta_{m-1}$, ne peut acquérir que $1.2.3\ldots(m-2)$ valeurs, par les $1.2.3\ldots(m-2)$ permutations des lettres $x_3, x_4, \ldots, x_m$.

En effet, si l'on remplace α par l'une quelconque de ses puissances, α^{n-1}, les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$ ne feront que s'échanger les unes dans les autres, car θ_2, θ_3, etc., se déduisant de θ_1 par les changements de α en α^2, α^3, etc., on peut les représenter par

$$(7) \qquad \theta(\alpha), \quad \theta(\alpha^2), \quad \theta(\alpha^3), \ldots, \quad \theta(\alpha^{m-1});$$

et ces quantités (7) sont évidemment les mêmes, à l'ordre près, que les suivantes :

$$(8) \qquad \theta(\alpha^{n-1}), \quad \theta[\alpha^{2(n-1)}], \ldots, \quad \theta[\alpha^{(m-1)(n-1)}].$$

Cela posé, le changement de α en α^{n-1} dans θ_1 ou $\theta(\alpha)$ équivaut à une certaine permutation des lettres $x_2, x_3, \ldots, x_m$, qui amène x_2 à la place de x_n; le même changement de α en α^{n-1}, ou de α^2 en $\alpha^{2(n-1)}$ dans θ_2 ou $\theta(\alpha^2)$, équivaut à la même permutation des lettres $x_2, x_3, \ldots, x_m$; et ainsi de suite; d'où il résulte que les quantités (8) se déduiront, à l'ordre près, des quantités (7) par la même substitution. Il y a donc, en un mot, une substitution qui peut amener x_2 à la place de l'une quelconque des lettres suivantes $x_3, x_4, \ldots, x_m$, et par laquelle les quantités θ_1,

$\theta_2, \ldots, \theta_{m-1}$ ne font que s'échanger les unes dans les autres. Par conséquent, cette substitution ne changera pas la valeur d'une fonction symétrique des quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$.

Supposons maintenant qu'on veuille appliquer à une fonction symétrique de θ_1, θ_2, etc., une substitution quelconque devant amener x_2 à la place de x_n, on pourra commencer par amener x_2 à la place de x_n par une substitution qui ne change en rien la valeur de la fonction symétrique, ensuite il n'y aura plus qu'à opérer une certaine substitution sur les $m-2$ lettres $x_3, x_4, \ldots, x_m$, la seule qui puisse changer la valeur de la fonction symétrique. Ainsi, la place de x_2 pouvant être fixée à volonté dans une fonction symétrique de θ_1, θ_2, etc., une pareille fonction ne saurait avoir que les $1.2.3\ldots(m-2)$ valeurs résultant des permutations des $m-2$ lettres x_3, $x_4, \ldots, x_m$.

D'après ce qui précède, chacun des coefficients P_1, P_2, etc., de l'équation (6) dépend d'une équation du degré $1.2.3\ldots(m-2)$, et l'on pourra former chacune de ces équations par la méthode exposée dans la troisième leçon, puisqu'on connaît la composition de leurs racines. Mais on aperçoit immédiatement que tous ces coefficients P_1, P_2, etc., ne dépendent que d'une seule équation du degré $1.2.3\ldots(m-2)$, car ce sont évidemment des fonctions semblables des racines $x_1, x_2, \ldots, x_m$ de l'équation proposée, et si l'on se donne la valeur de l'un d'eux, celles de tous les autres s'en déduiront rationnellement.

Voici comment on peut opérer pour former l'équation dont P_1 dépend, et pour exprimer en fonction de P_1 les autres coefficients P_2, P_3, etc. On calculera l'équation de degré $1.2.3\ldots(m-1)$, qui a pour racines toutes les valeurs de θ et dont les coefficients, fonctions invariables des racines de la proposée, sont exprimables rationnelle-

ment par ses coefficients. Le premier membre de l'équation (6) étant un diviseur du premier membre de cette équation complète en θ, on fera la division à la manière ordinaire, et on égalera à zéro les $m-1$ termes du reste. Les $m-2$ premières des équations ainsi obtenues serviront à déterminer les coefficients P_2, P_3, etc., en fonction de P_1, et on aura ensuite l'équation en P_1 de degré $1.2.3\ldots(m-2)$, en remplaçant dans la $(m-1)^{ième}$, P_2, P_3, etc., par les valeurs qu'on aura trouvées.

Lagrange a cherché à simplifier les calculs, presque impraticables dès le cinquième degré, auxquels conduit l'application de la théorie précédente; il a effectivement imaginé un artifice ingénieux pour exprimer les coefficients de l'équation (6), en fonction des racines x_1, x_2, etc. Je vais le rapporter ici.

Pour avoir l'expression de θ, il faut élever à la puissance m la quantité

$$x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m;$$

en faisant ce calcul, et ayant soin de rabaisser les exposants de α au-dessous de m, on a un résultat de la forme

$$(9) \qquad \theta = \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \ldots + \alpha^{m-1}\xi_{m-1}.$$

L'équation (9) donne les valeurs de $\theta_1, \theta_2, \ldots, \theta_{m-1}$, en substituant à α chacune des racines imaginaires α, 6, $\gamma, \ldots, \omega$ de l'équation $x^m = 1$. En outre, si l'on remplace α par 1, le second membre de l'équation (9) a pour valeur $(x_1 + x_2 + \ldots + x_m)^m$ ou A^m, en désignant par A la somme connue des racines de l'équation proposée (1). On a donc

$$\begin{aligned}
A^m &= \xi_0 + \xi_1 + \xi_2 + \ldots + \xi_{m-1},\\
\theta_1 &= \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \ldots + \alpha^{m-1}\xi_{m-1},\\
\theta_2 &= \xi_0 + 6\xi_1 + 6^2\xi_2 + \ldots + 6^{m-1}\xi_{m-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\theta_{m-1} &= \xi_0 + \omega\xi_1 + \omega^2\xi_2 + \ldots + \omega^{m-1}\xi_{m-1}.
\end{aligned}$$

Ajoutons ces équations et désignons par S_1 la somme des racines de l'équation (6); on aura, d'après les propriétés des racines α, 6, etc.,

$$A^m + S_1 = m\,\xi_0,$$

ou

$$S_1 = m\,\xi_0 - A^m.$$

Désignons généralement par S_n la somme des puissances n des racines de l'équation (6); élevons l'équation (9) à la puissance n, et rabaissant les exposants de α au-dessous de m, représentons le résultat par

$$\theta^n = \xi_0^{(n)} + \alpha\xi_1^{(n)} + \alpha^2\xi_2^{(n)} + \ldots + \alpha^{m-1}\xi_{m-1}^{(n)};$$

remplaçons ensuite α successivement par $1, \alpha, 6, \ldots, \omega$, et ajoutons les résultats, on aura

$$A^{mn} + S_n = m\,\xi_0^{(n)},$$

ou

$$S_n = m\,\xi_0^{(n)} - A^{mn}.$$

On pourra calculer de cette manière, en fonction des racines $x_1, x_2, \ldots, x_m$, les sommes $S_2, S_3, \ldots, S_{m-1}$, et l'on en déduira ensuite les valeurs suivantes des coefficients P_1, P_2, etc., de l'équation (6)

$$P_1 = -\,(m\,\xi_0 - A^m),$$

$$P_2 = -\frac{(m\,\xi_0 - A^m)^2}{2} - \frac{(m\,\xi_0^{(2)} - A^{2m})}{2},$$

$$P_3 = -\frac{(m\,\xi_0 - A^m)^3}{2.3} + \frac{(m\,\xi_0 - A^m)(m\,\xi_0^{(2)} - A^{2m})}{2} - \frac{(m\,\xi_0^{(3)} - A^{3m})}{3},$$

....

....

Voilà donc les coefficients P_1, P_2, etc., de l'équation (6) exprimés en fonction des racines $x_1, x_2, \ldots, x_m$ de l'équation proposée, et si l'on fait dans l'expression de l'un d'eux, de P_1 par exemple, toutes les permutations possibles, on ne trouvera que $1.2.3\ldots(m-2)$ valeurs distinctes. On pourra ainsi former directement l'équation en P_1, et l'on exprimera ensuite les valeurs des autres coefficients en fonction rationnelle de P_1, par le procédé indiqué plus haut.

Si l'on connaît un seul système de valeurs des coefficients P_1, P_2, etc., et si l'on peut résoudre l'équation en θ correspondante de degré $m-1$, la résolution de l'équation proposée (1) s'ensuivra immédiatement, comme nous allons l'expliquer

Dans l'hypothèse où nous nous plaçons, les quantités $\theta_1, \theta_2, \ldots, \theta_{m-1}$ sont connues : les équations (5) donnent, en mettant $\alpha, \beta, \gamma, \ldots, \omega$ au lieu de $\alpha, \alpha^2, \ldots, \alpha^{m-1}$,

$$(10)\quad \left\{\begin{array}{l} x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m = \sqrt[m]{\theta_1}, \\ x_1 + \beta x_2 + \beta^2 x_3 + \ldots + \beta^{m-1} x_m = \sqrt[m]{\theta_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{m-1} x_m = \sqrt[m]{\theta_{m-1}}, \end{array}\right.$$

on a d'ailleurs

$$x_1 + x_2 + x_3 + \ldots + x_m = A;$$

donc, en ajoutant ces équations, et ayant égard aux propriétés des racines α, β, etc., on a

$$(11)\qquad x_1 = \frac{A + \sqrt[m]{\theta_1} + \sqrt[m]{\theta_2} + \ldots + \sqrt[m]{\theta_{m-1}}}{m};$$

ajoutant aussi ces mêmes équations respectivement mul-

tipliées par α^n, 6^n, ..., ω^n et 1, on a

$$(12)\qquad x_{m-n+1} = \frac{A + \alpha^n \sqrt[m]{\theta_1} + 6^n \sqrt[m]{\theta_2} + \ldots + \omega^n \sqrt[m]{\theta_{m-1}}}{m}.$$

Mais comme rien ne détermine celle des valeurs de chaque radical qu'il faut prendre, le second membre de l'équation (12) est absolument identique au second membre de l'équation (11). Aussi doit-on se borner à dire que les m racines de l'équation proposée sont données par la formule unique

$$(13)\qquad x = \frac{A + \sqrt[m]{\theta_1} + \sqrt[m]{\theta_2} + \ldots + \sqrt[m]{\theta_{m-1}}}{m}.$$

A la vérité, cette formule, à cause de la multiplicité des valeurs de chaque radical, donne pour x un nombre de valeurs égal à m^{m-1}; mais on peut faire disparaître l'ambiguïté qui en résulte. En effet, les premiers membres des équations (10) sont des fonctions semblables des racines x_1, x_2, etc.; on pourra donc, si l'on se donne l'un d'eux, en déduire rationnellement tous les autres. Ainsi, on pourra exprimer $\sqrt[m]{\theta_2}$, $\sqrt[m]{\theta_3}$, ..., $\sqrt[m]{\theta_{m-1}}$ rationnellement en fonction de $\sqrt[m]{\theta_1}$, et la formule (13) ne donnera alors pour x que m valeurs, comme cela doit être.

Par cette méthode, la résolution de l'équation du cinquième degré se ramène à celle d'une équation du quatrième degré, dont les coefficients dépendent d'une équation du sixième.

Des équations de degré non premier.

On voit aisément que l'analyse précédente ne peut s'appliquer aux équations dont le degré est un nombre composé. En effet, les quantités θ_1, θ_2, etc., que nous avons

déduites de θ en remplaçant α successivement par α, α^2, α^3, etc., ne sont plus toutes des racines de l'équation résolvante en θ, parce qu'alors, en remplaçant α par l'une de ces puissances dans la série

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,$$

on ne reproduit pas nécessairement ces mêmes quantités, lors même que α serait une racine primitive de l'équation $x^m = 1$. Aussi Lagrange a-t-il cherché une autre méthode : celle qu'il a suivie revient, en dernière analyse, à décomposer l'équation proposée

(1) $$V = 0,$$

de degré $m = np$, n étant un nombre premier, en n équations du degré p; et cette méthode n'exige pour cela que la résolution d'une équation du degré

$$\frac{1.2\ldots m}{(n-1)\,n\,(1.2\ldots p)^n},$$

et celle d'une équation de degré $n-1$, tandis que si l'on cherchait à faire la décomposition par la méthode ordinaire, il faudrait résoudre une équation du degré

$$\frac{m(m-1)\ldots(m-p+1)}{1.2\ldots p}.$$

Cette décomposition de l'équation (1) en n équations du degré p une fois faite, on pourra appliquer à chacune de ces dernières la méthode exposée précédemment, si p est un nombre premier. Dans le cas contraire, si $p = n'p'$, n' étant un nombre premier, on ramènera la résolution de chaque équation de degré p à celle de n' équations du degré p', en opérant de la même manière que pour la proposée; et ainsi de suite. Entrons maintenant dans les détails.

Soit $m = np$, n étant un nombre premier, et posons, comme précédemment,

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{m-1} x_m,$$

$x_1, x_2, \ldots, x_m$ désignant les m racines de l'équation (1) et α une racine de $x^m = 1$, mais qui appartienne aussi à l'équation $x^n = 1$. Alors, comme on a généralement

$$\alpha^{n+k} = \alpha^k,$$

la valeur précédente de t pourra s'écrire comme il suit :

$$\begin{aligned} t = {} & [x_1 + x_{n+1} + x_{2n+1} + \ldots + x_{(p-1)n+1}] \\ & + \alpha[x_2 + x_{n+2} + x_{2n+2} + \ldots + x_{(p-1)n+2}] \\ & + \ldots\ldots\ldots\ldots\ldots\ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & + \alpha^{n-1}[x_n + x_{2n} + x_{3n} + \ldots\ldots + x_{pn}], \end{aligned}$$

ou

$$t = X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{n-1} X_n,$$

en faisant, pour abréger,

$$(2)\quad \begin{cases} X_1 = x_1 + x_{n+1} + x_{2n+1} + \ldots + x_{(p-1)n+1}, \\ X_2 = x_2 + x_{n+2} + x_{2n+2} + \ldots + x_{(p-1)n+2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ X_n = x_n + x_{2n} + x_{3n} + \ldots\ldots + x_{pn}. \end{cases}$$

Soit

$$(3)\qquad W = 0$$

l'équation qui a pour racines $X_1, X_2, \ldots, X_n$; on pourra appliquer à cette équation (3) la méthode exposée précédemment pour les équations de degré premier. Faisons $\theta = t^n$, ou

$$(4)\qquad \theta = (X_1 + \alpha X_2 + \ldots + \alpha^{n-1} X_n)^n;$$

θ dépend d'une équation du degré 1.2.3... $(n-1)$ dont les coefficients peuvent s'exprimer rationnellement par ceux de l'équation (3); et si l'on représente par $\theta_1, \theta_2, \ldots, \theta_{n-1}$, les $n-1$ valeurs que prend θ, quand on remplace α par les $n-1$ racines imaginaires de $x^n = 1$, on pourra former l'équation de degré $n-1$ qui a ces $n-1$ valeurs de θ pour racines : représentons cette équation par

$$(5) \qquad \theta^{n-1} + P_1\theta^{n-2} + P_2\theta^{n-3} + \ldots + P_{n-2}\theta + P_{n-1} = 0;$$

ses coefficients P_1, P_2, etc., dépendent d'une seule équation de degré 1.2.3... $(n-2)$ dont les coefficients s'expriment rationnellement par ceux de l'équation (3), ainsi que nous l'avons établi précédemment.

Soient y l'un quelconque des coefficients P_1, P_2, etc., et

$$(6) \qquad f(y) = 0$$

l'équation de degré 1.2.3... $(n-2)$ dont y dépend. Les coefficients de cette équation (6) sont exprimables rationnellement par ceux de l'équation (3), mais ces derniers ne sont pas connus, il n'y a que ceux de l'équation (1) qui le soient; voici comment on peut former une équation en y dont les coefficients soient exprimés par les quantités connues.

$f(y)$ est une fonction de y qui contient symétriquement les quantités $X_1, X_2, \ldots, X_n$, et, en remplaçant X_1, X_2, etc., par leurs valeurs tirées des équations (2), $f(y)$ deviendra une fonction non symétrique des racines $x_1, x_2, \ldots, x_m$ de l'équation (1). Faisons dans $f(y)$ toutes les permutations des racines $x_1, x_2, \ldots, x_m$, et désignons par

$$f_1(y), \quad f_2(y), \ldots, f_\mu(y)$$

les μ valeurs distinctes que prend ainsi $f(y)$; le produit

de toutes ces valeurs est une fonction symétrique des racines $x_1, x_2, \ldots, x_m$ de la proposée, exprimable rationnellement par ses coefficients. On a donc, pour déterminer y, l'équation

$$(7) \qquad f_1(y) f_2(y) f_3(y) \ldots f_\mu(y) = 0,$$

dont les coefficients peuvent être considérés comme connus.

Le degré de cette équation (7) est $1.2.3\ldots(n-2) \times \mu$, μ désignant le nombre des valeurs distinctes que prend $f(y)$, quand on y permute les lettres $x_1, x_2, \ldots, x_m$; nous savons que ce nombre μ est un diviseur du produit $1.2.3\ldots m$ (onzième leçon), et si l'on fait

$$\mu = \frac{1.2.3\ldots m}{\nu},$$

ν sera le nombre des permutations des lettres $x_1, x_2, \ldots, x_m$ qui ne font pas changer la fonction $f(y)$. Or $f(y)$ ne change pas en changeant, les unes dans les autres, les lettres qui composent respectivement $X_1, X_2, \ldots, X_n$, non plus qu'en échangeant les quantités X_1, X_2, etc., les unes dans les autres; mais toute permutation des lettres x_1, x_2, etc., qui fait passer quelques-unes des lettres de X_1, ou X_2, ou, etc., dans l'une des autres fonctions, change évidemment la fonction $f(y)$. On conclut aisément de là que

$$\nu = (1.2.3\ldots p)^n.(1.2\ldots n),$$

et, par conséquent,

$$\mu = \frac{1.2.3\ldots m}{(1.2.3\ldots n).(1.2.3\ldots p)^n}.$$

Le degré de l'équation (7) est donc

$$1.2.3\ldots(n-2).\frac{1.2.3\ldots m}{(1.2.3\ldots n)(1.2\ldots p)^n},$$

ou

$$\frac{1.2.3\ldots m}{(n-1)\,n\,(1.2.3\ldots p)^n}.$$

Si l'on connaît une seule racine de l'équation (7), on aura un système de valeurs des coefficients

$$P_1,\ P_2,\ldots,\ P_{n-1}$$

de l'équation (5), car ces coefficients sont des fonctions semblables des racines de l'équation proposée, et, par conséquent, ils peuvent s'exprimer rationnellement en fonction de l'un quelconque d'entre eux et des quantités connues.

On résoudra ensuite l'équation (5), qui n'est que du degré $n-1$, et l'on aura alors aisément les racines de l'équation (3). Désignons, en effet, par

$$\theta_1,\ \theta_2,\ldots,\theta_{n-1}$$

les $n-1$ racines de l'équation (5); ces valeurs de θ étant précisément celles qu'on déduit de l'équation (4), en remplaçant α par chacune des racines imaginaires de $x^n = 1$, on aura

$$X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{n-1} X_n = \sqrt[n]{\theta_1},$$
$$X_1 + 6 X_2 + 6^2 X_3 + \ldots + 6^{n-1} X_n = \sqrt[n]{\theta_2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$X_1 + \omega X_2 + \omega^2 X_3 + \ldots + \omega^{n-1} X_n = \sqrt[n]{\theta_{n-1}}.$$

D'ailleurs, la somme des racines $X_1,\ X_2,\ldots,\ X_n$ est

connue, car elle est la même que celles des racines x_1, $x_2, \ldots, x_m$; en désignant donc par A cette somme, on aura

$$X_1 + X_2 + X_3 + \ldots + X_n = A.$$

Des équations qui précèdent, on tire cette expression générale des racines X_1, X_2, etc.,

$$X = \frac{A + \sqrt[n]{\theta_1} + \sqrt[n]{\theta_2} + \ldots + \sqrt[n]{\theta_{n-1}}}{n}.$$

Il ne reste plus, maintenant, qu'à trouver les racines x_1, x_2, etc., elles-mêmes; pour cela, on considérera l'équation qui a pour racines celles de la proposée dont la somme est X_1 ou X_2, ou etc., X_1 par exemple: soit

$$x^p - X_1 x^{p-1} + Q_2 x^{p-2} + \ldots + Q_{p-1} x + Q_p = 0$$

cette équation, dont le premier membre est un diviseur du premier membre V de la proposée. On fera la division à la manière ordinaire, et on égalera à zéro les p termes du reste; on aura ainsi p équations dont les $p - 1$ premières détermineront Q_2, Q_3, etc., en fonction de X_1, la dernière étant alors satisfaite d'elle-même. Il est évident, à priori, que Q_2, Q_3, etc., doivent s'exprimer rationnellement en fonction de X_1, puisque ce sont des fonctions semblables. On aura donc enfin, par ce moyen, les n équations de degré p, dans lesquelles peut se décomposer l'équation proposée.

Tel est le point où se trouve ramenée aujourd'hui la question de la résolution algébrique des équations. La fonction résolvante de Lagrange nous a donné la résolution des équations du troisième et du quatrième degré, mais elle n'est d'aucune utilité pour les équations géné-

rales de degré supérieur au quatrième, dont, au surplus, la résolution est aujourd'hui demontrée impossible. Toutefois nous verrons, dans une prochaine leçon, que la considération de cette fonction résolvante conduit à la résolution algébrique d'une classe fort étendue d'équations de degrés quelconques.

A la même époque où Lagrange publiait, à Berlin, le Mémoire dont nous venons de présenter les résultats principaux, Vandermonde s'occupait de la même question, et présentait, à l'Académie des Sciences de Paris, un beau Mémoire où, par des considérations différentes de celles de Lagrange, il arrivait pourtant aux mêmes conséquences. Je me borne ici à indiquer ce travail de Vandermonde, imprimé dans les *Mémoires de l'Académie des Sciences de Paris* (année 1771).

DIX-NEUVIÈME LEÇON.

Sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. — Des substitutions circulaires. — Théorème de M. Cauchy. — Forme generale des fonctions qui ont deux valeurs.

Sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme.

Le succès des méthodes exposées précédemment pour la résolution des équations générales du troisième et du quatrième degré est dû à cette seule circonstance, qu'on peut former des fonctions de trois lettres qui n'aient que deux valeurs, et des fonctions de quatre lettres qui n'en aient que trois. Et si l'on pouvait de même former des fonctions de cinq lettres n'ayant que quatre ou trois valeurs, on est fondé à penser que ces fonctions permettraient de résoudre l'équation générale du cinquième degré. On voit par là combien la question du nombre de valeurs qu'une fonction rationnelle peut acquérir, quand on y permute les lettres qu'elle renferme, est liée intimement à la théorie des équations. Aussi plusieurs géomètres s'en sont-ils occupés, et quoiqu'ils aient laissé beaucoup à faire après eux, ils ont pourtant obtenu quelques résultats intéressants que nous allons exposer.

Lagrange est le premier qui se soit occupé de cette question, en démontrant (*voir* onzième leçon) que *le nombre des valeurs d'une fonction de n lettres est toujours un diviseur du produit* $1.2.3\ldots n$.

Rufini, dans sa Théorie des équations, a considéré par-

ticulièrement les fonctions de cinq lettres, et il est parvenu à démontrer le théorème suivant :

Si une fonction de cinq lettres a moins de cinq valeurs distinctes, elle ne peut en avoir plus de deux.

M. Cauchy, dans un Mémoire qui fait partie du x[e] cahier du *Journal de l'École Polytechnique,* a démontré ensuite un théorème plus général et qui consiste en ce que :

Si une fonction de n lettres a moins de p valeurs distinctes (p étant le plus grand nombre premier contenu dans n), elle ne peut en avoir plus de deux.

Et comme $p = n$, si n est premier, on a, en particulier, ce théorème :

Si une fonction de n lettres a moins de n valeurs distinctes, n étant un nombre premier, elle ne peut en avoir plus de deux.

M. Cauchy donne à entendre, dans son Mémoire, qu'il chercha à étendre le théorème précédent au cas où n n'est pas un nombre premier, mais il ne put y parvenir que dans le cas de $n = 6$. Il a, en effet, démontré que

Si une fonction de six lettres a moins de six valeurs distinctes, elle ne peut en avoir plus de deux.

Enfin M. Bertrand s'est occupé, dans ces dernières années, de cette même question, et il est parvenu à démontrer généralement le théorème que M. Cauchy avait établi, avant lui, dans un cas particulier (*). Ainsi, d'après M. Bertrand,

Si une fonction de n lettres a moins de n valeurs distinctes, elle ne peut en avoir plus de deux.

La démonstration de M. Bertrand repose sur le *postulatum* suivant : *Si l'on a $n > 7$, il y a au moins un nombre premier p compris entre $n - 2$ et $\frac{n}{2}$.* Les Tables

(*) *Journal de l'École Polytechnique,* xxx[e] cahier.

de nombres premiers ont permis de constater l'exactitude de ce *postulatum* pour toutes les valeurs de n comprises entre 7 et 6 000 000, en sorte que le théorème de M. Bertrand se trouve démontré par lui pour les fonctions qui ont moins de 6 000 000 de variables. Au surplus, le postulatum dont il s'agit a été démontré rigoureusement dans ces derniers temps par un habile géomètre de Saint-Pétersbourg, M. Tchebicheff. (*Voir* la Note XV.)

Le raisonnement dont M. Bertrand a fait usage, conduit à cet autre théorème, démontré auparavant par Abel pour les fonctions de cinq lettres :

Si une fonction de n lettres a n valeurs, elle est symétrique par rapport à n — 1 lettres.

Dans une Note publiée dans le XXXIIe cahier du *Journal de l'École Polytechnique*, j'ai fait voir que si, entre $n-2$ et $\frac{n}{2}$, il n'y a aucun nombre premier, le théorème de M. Bertrand continue d'avoir lieu, pourvu que $\frac{n}{2}$ soit un nombre premier. La démonstration n'est en aucune façon modifiée; seulement on ne peut plus conclure ce corollaire, que si une fonction de n lettres a n valeurs, elle est symétrique par rapport à $n-1$ lettres.

Cette remarque est importante, car il en résulte que le théorème de M. Bertrand comprend celui de M. Cauchy pour les fonctions de six lettres, et rend, par suite, inutile la démonstration un peu compliquée de M. Cauchy. En effet, si $n=6$, il n'y a aucun nombre premier entre $n-2$ et $\frac{n}{2}$; mais $\frac{n}{2}$ ou 3 est un nombre premier.

M. Bertrand a démontré aussi, dans son Mémoire, le théorème suivant :

Si une fonction de n lettres, n étant >9, *a plus de n valeurs, elle en a au moins 2 n.*

Tels sont les résultats principaux acquis à la science

dans cette théorie (*). Le problème général, qu'il serait intéressant de résoudre, consisterait à déterminer quels sont, parmi les diviseurs du produit $1.2.3\ldots n$, ceux qui peuvent représenter le nombre des valeurs d'une fonction de n lettres. On voit combien les théorèmes que nous venons d'indiquer sont loin de répondre, d'une manière complète, à cette question. Toutefois ces théorèmes suffisent pour l'objet qu'on doit avoir en vue dans la théorie des équations. Ainsi, en particulier, le théorème de Rufini, s'il n'établit pas l'impossibilité de résoudre l'équation générale du cinquième degré, prouve du moins l'impossibilité de former une résolvante dont le degré soit inférieur à cinq.

Des substitutions circulaires.

Pour bien comprendre les développements dans lesquels nous allons entrer, il est nécessaire de se faire une idée précise de l'opération que nous avons désignée par le mot de *substitution* (*voir* onzième leçon).

Soit

$$F(a, b, c, \ldots, k, l)$$

(*) Dans un Mémoire que j'ai présenté à l'Académie des Sciences le 2 juillet 1849, j'ai démontré, sans avoir recours à aucun postulatum, les théorèmes suivants :

1°. Une fonction de n lettres qui a moins de n valeurs n'en a que deux au plus, à moins que n ne soit égal à 4;

2°. Une fonction de n lettres qui a précisément n valeurs est symétrique par rapport à $n-1$ lettres, à moins que n ne soit égal à 6;

3°. Une fonction de n lettres qui a plus de n valeurs en a au moins $2n$ si n est > 8;

4°. Une fonction de n lettres qui a plus de $2n$ valeurs en a au moins $\frac{n(n-1)}{2}$ si n est > 12.

La méthode dont j'ai fait usage dans ces recherches diffère essentiellement de celles qui avaient été employées jusqu'ici. On trouvera un extrait de mon Mémoire dans la Note VIII.

une fonction de n lettres. Si, parmi ces n lettres, on en prend p au hasard,

$$a, b, c, \ldots, g$$

par exemple, et qu'après les avoir rangées en cercle on mette chacune d'elles à la place de celle qui la précède, on dit que l'on a fait subir à ces p lettres une permutation circulaire, et la substitution

$$\begin{pmatrix} a, b, c, \ldots, g \\ b, c, \ldots, g, a \end{pmatrix}$$

est dite une substitution circulaire de l'*ordre* p. Cela posé, on a le théorème suivant :

Théorème. — *Toute substitution, si elle n'est pas circulaire, équivaut à plusieurs substitutions circulaires effectuées simultanément sur des lettres différentes.*

Supposons, en effet, que l'on fasse subir une substitution quelconque aux lettres

$$a, b, c, \ldots, f, g;$$

par cette substitution, a se trouve remplacée par une certaine lettre, c par exemple, c elle-même sera remplacée par une troisième lettre e, et, en continuant de cette manière, on tombera nécessairement sur une lettre qui se trouvera remplacée par a. Or il est évident que les lettres que l'on a ainsi rencontrées ont subi une permutation circulaire. En prenant une des lettres restantes, et opérant de la même manière, on formera un nouveau groupe de lettres qui auront subi également une permutation circulaire, et ainsi de suite, jusqu'à ce que toutes les lettres soient épuisées.

Le raisonnement dont nous venons de faire usage donne le moyen de former immédiatement les substitutions circulaires qui équivalent à une substitution don-

née. Considérons, par exemple, la substitution

$$\begin{pmatrix} a, b, c, d, e, f, g, h, i, j, o \\ h, o, d, f, b, j, a, g, e, c, i \end{pmatrix},$$

on trouvera qu'elle équivaut aux trois substitutions circulaires suivantes :

$$\begin{pmatrix} a, h, g \\ h, g, a \end{pmatrix} \begin{pmatrix} b, o, i, e \\ o, i, e, b \end{pmatrix} \begin{pmatrix} c, d, f, j \\ d, f, j, c \end{pmatrix}.$$

Le même procédé doit aussi être employé quand on veut reconnaître si une substitution est circulaire ou non. Ainsi on trouvera que la substitution

$$\begin{pmatrix} a, b, c, d, e, f, g, h, i, j, o \\ g, d, f, j, a, o, c, i, b, e, h \end{pmatrix}$$

est circulaire, car on peut l'écrire de la manière suivante :

$$\begin{pmatrix} a, g, c, f, o, h, i, b, d, j, e \\ g, c, f, o, h, i, b, d, j, e, a \end{pmatrix}.$$

Si, après avoir effectué une substitution circulaire sur p lettres, on répète $1, 2, 3, \ldots, p-1$ fois la même substitution, on obtiendra p arrangements différents; mais en faisant une fois de plus cette substitution, on reproduira l'arrangement primitif.

Nous désignerons par le mot *transposition* la substitution circulaire de deux lettres, c'est-à-dire l'opération qui consiste à échanger simplement ces deux lettres l'une avec l'autre, et nous indiquerons par la notation abrégée (a, b) la transposition des lettres a et b.

Il est évident que toute substitution, circulaire ou non, équivaut à une série de transpositions. Car supposons qu'il s'agisse d'opérer une substitution quelconque sur les lettres

$$a, b, c, \ldots, f, g,$$

on amènera a à la nouvelle place qu'elle doit occuper par

une transposition; cela fait, une autre transposition amènera b à la place qu'elle doit occuper, et ainsi de suite, jusqu'à ce que toutes les lettres aient pris les places qu'on veut leur donner.

Théorème de M. Cauchy.

La démonstration du théorème de M. Cauchy repose sur les quatre lemmes suivants :

LEMME Ier. — *Si une fonction de n lettres n'est pas changée par une substitution circulaire effectuée sur p lettres, elle ne changera pas non plus en répétant cette substitution un nombre quelconque de fois.*

Ce lemme est presque évident; car, soit la fonction

$$F(a, b, c, d, e, \ldots),$$

et supposons que cette fonction ne soit pas changée par la substitution circulaire du cinquième ordre

$$\begin{pmatrix} a, & b, & c, & d, & e \\ b, & c, & d, & e, & a \end{pmatrix},$$

on aura

$$F(a, b, c, d, e, \ldots) = F(b, c, d, e, a, \ldots);$$

mais cette égalité ayant lieu quelles que soient les quantités représentées par a, b, c, d, e, on aura aussi

$$\begin{aligned} F(b, c, d, e, a, \ldots) &= F(c, d, e, a, b, \ldots), \\ F(c, d, e, a, b, \ldots) &= F(d, e, a, b, c, \ldots), \\ F(d, e, a, b, c, \ldots) &= F(e, a, b, c, d, \ldots), \\ F(e, a, b, c, d, \ldots) &= F(a, b, c, d, e, \ldots); \end{aligned}$$

car chacune de ces égalités se déduit de celle qui a lieu par hypothèse, en représentant par d'autres lettres les quantités actuellement représentées par a, b, c, d, e.

Le même raisonnement montre que si une fonction

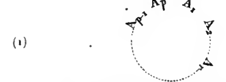
n'est pas changée en faisant r fois de suite une permutation circulaire de p lettres, elle ne changera pas non plus en répétant $2r$ fois, $3r$ fois, etc., cette même permutation circulaire.

LEMME II. — *Réciproquement, si p est un nombre premier, et si une fonction de n lettres n'est pas changée en opérant une substitution circulaire de p lettres, un certain nombre de fois inférieur à p, cette fonction ne changera pas non plus, en faisant une seule fois la substitution circulaire.*

Désignons par A_1 une permutation formée avec p des n lettres de la fonction donnée, et appliquons $p-1$ fois à la permutation A_1, une même substitution circulaire d'ordre p. On aura de cette manière p permutations que nous représenterons par

$$A_1,\ A_2,\ A_3, \ldots,\ A_p,$$

ou, en les rangeant en cercle, par

(1) 

Si maintenant la permutation A_1 donne à la fonction la même valeur que la permutation A_r, on pourra, d'après le lemme I, répéter un nombre quelconque de fois la substitution par laquelle on passe de la permutation A_1 à la permutation A_r. Or, pour avoir les permutations correspondantes, il suffit de joindre de r en r les sommets du polygone (1), et comme p est un nombre premier, on sait qu'on ne reviendra au point de départ qu'après avoir rencontré tous les sommets; d'où il résulte que les per-

mutations

$$A_1,\ A_2,\ldots,\ A_p$$

donnent la même valeur à la fonction.

LEMME III. — *Si une fonction n'est changée par aucune substitution circulaire opérée sur p lettres, elle ne sera pas changée non plus par une substitution circulaire opérée sur trois lettres quelconques.*

Soit

$$(1)\qquad \begin{pmatrix} a, b, c, d, \ldots, k, l \\ b, c, d, \ldots, k, l, a \end{pmatrix}$$

une substitution circulaire d'ordre p; la substitution

$$(2)\qquad \begin{pmatrix} b, c, d, \ldots, k, l, a \\ c, a, b, d, \ldots, k, l \end{pmatrix}$$

sera également circulaire. En effet, en opérant, comme il a été indiqué au commencement de cette leçon, on peut écrire cette substitution de la manière suivante :

$$\begin{pmatrix} b, c, a, l, \ldots, d \\ c, a, l, k, \ldots, b \end{pmatrix}.$$

Donc, puisque, par hypothèse, la fonction qu'on considère n'est changée par aucune substitution circulaire de p lettres, on pourra, sans changer sa valeur, lui appliquer successivement les deux substitutions (1) et (2), ou, ce qui revient au même, la substitution unique

$$\begin{pmatrix} a, b, c, d, \ldots, k, l \\ c, a, b, d, \ldots, k, l \end{pmatrix}.$$

Mais cette dernière revient simplement à remplacer les trois lettres a, b, c, par c, a, b; la fonction ne sera donc pas changée par la substitution

$$\begin{pmatrix} a, b, c \\ c, a, b \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} a, c, b \\ c, b, a \end{pmatrix},$$

qui est circulaire et qui doit être effectuée sur trois lettres *quelconques*.

LEMME IV. — *Si une fonction n'est changée par aucune substitution circulaire de trois lettres, elle n'a au plus que deux valeurs.*

Toute substitution circulaire de trois lettres équivaut à deux transpositions opérées successivement. Ainsi la substitution

$$\begin{pmatrix} a, & b, & c \\ b, & c, & a \end{pmatrix}$$

revient à opérer d'abord la transposition (a, b), puis ensuite la transposition (a, c), qui a une lettre commune a avec la première. Ainsi, dire qu'une fonction n'est changée par aucune substitution circulaire de trois lettres, c'est dire qu'elle n'est pas changée par deux transpositions ayant une lettre commune, opérées successivement.

Soit donc V une fonction de n lettres a, b, c, d, etc., qui n'est changée par aucune substitution circulaire de trois lettres. D'après ce qui précède, V ne changera pas en opérant successivement deux transpositions (a, b), (a, c), ayant une lettre commune. Supposons que V devienne V_1 quand on lui applique la transposition (a, b), (V_1 pouvant être égal à V), la transposition (a, c) devra changer V_1 en V, et, par suite, V en V_1; car, faire deux fois de suite une transposition, c'est ne faire aucun changement. Il résulte de là que deux transpositions (a, b), (a, c), qui ont une lettre commune, produisent le même changement dans la fonction; il en sera de même des deux transpositions (a, c), (c, d) et, par suite, des deux transpositions (a, b), (c, d) qui n'ont aucune lettre commune.

Cela posé, toute substitution équivalant à plusieurs transpositions, on voit que V n'a au plus que deux valeurs; car si une première transposition change V en V_1,

une deuxième changera V_1 en V, une troisième V en V_1, et ainsi de suite ; en sorte que V n'aura que deux valeurs, et elle n'en aura même qu'une seule si $V = V_1$.

Théorème de M. Cauchy. — *Si une fonction de n lettres a moins de p valeurs, p étant le plus grand nombre premier contenu dans n, elle ne peut avoir plus de deux valeurs.*

Soient V une fonction de n lettres, p un nombre premier égal ou inférieur à n, et supposons que la fonction V ait moins de p valeurs.

Parmi les n lettres de la fonction V, prenons-en p au hasard, formons avec ces p lettres un premier arrangement A_1, puis faisons subir aux p lettres de cet arrangement, $p - 1$ fois de suite, une même substitution circulaire d'ordre p ; on aura en tout p arrangements que nous désignerons par

$$A_1, \quad A_2, \quad A_3, \ldots, \quad A_p.$$

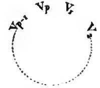
Appliquons à la fonction V les p substitutions

$$\begin{pmatrix} A_1 \\ A_1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} \begin{pmatrix} A_1 \\ A_3 \end{pmatrix} \cdots \begin{pmatrix} A_1 \\ A_p \end{pmatrix},$$

il en résultera p valeurs de V, que nous représenterons par

$$V_1, \quad V_2, \quad V_3, \ldots, \quad V_p,$$

ou, les rangeant en cercle, par



Or, par hypothèse, la fonction V a moins de p valeurs

distinctes; il y a donc au moins deux valeurs de V égales entre elles parmi celles que nous venons d'écrire. Supposons que l'on ait

$$V_{r+r'} = V_{r'};$$

alors la fonction $V_{r'}$ ne change pas quand on fait subir aux p lettres que nous avons considérées r fois de suite une substitution circulaire; elle ne changera donc pas, p étant un nombre premier, si l'on ne fait qu'une seule fois cette substitution (lemme II), et, par suite, si on la fait un nombre quelconque de fois (lemme I). Mais chaque valeur de V se déduit de la précédente par une substitution circulaire des p lettres considérées; donc les p valeurs de V sont égales entre elles.

Il résulte de là que la fonction V n'est changée par aucune substitution circulaire de p lettres; donc elle ne le sera pas non plus par une substitution circulaire de trois lettres quelconques (lemme III), et, par conséquent, elle n'a que deux valeurs au plus (lemme IV).

Corollaire I. — Si n est premier, on peut prendre $p = n$, et l'on a ce théorème : *Si une fonction de n lettres, (n étant premier), a moins de n valeurs, elle ne peut en avoir plus de deux.*

En particulier : *Si une fonction de cinq lettres a plus de deux valeurs, elle en a au moins cinq.*

Corollaire II. — *Toute fonction de n lettres qui n'a que deux valeurs n'est changée par aucune substitution circulaire de trois lettres, et, par conséquent, elle est changée par une transposition quelconque.*

En effet, d'après le théorème précédent, une fonction qui a moins de trois valeurs n'est changée par aucune substitution circulaire de trois lettres, et, d'après le lemme IV, toutes les transpositions produisent le même changement sur la fonction; sa valeur doit donc changer

par une transposition quelconque si elle n'est pas symétrique. Et, en général, une substitution quelconque change ou ne change pas la valeur de la fonction, suivant que cette substitution équivaut à un nombre pair ou impair de transpositions.

Forme générale des fonctions qui ont deux valeurs.

On peut toujours, quel que soit n, former des fonctions de n lettres qui n'aient que deux valeurs.

Considérons, en effet, les n lettres

$$a,\ b,\ c,\ldots,\ k,\ l,$$

et désignons par v le produit de toutes les différences obtenues, en retranchant de chacune de ces lettres successivement chacune des suivantes, on aura

$$v = (a-b)(a-c)\ldots(a-l)(b-c)\ldots(k-l).$$

Le carré de v est évidemment une fonction symétrique, et, par conséquent, v ne peut avoir que deux valeurs égales et de signes contraires. Ces deux valeurs existent effectivement; car on voit que v se change en $-v$ quand on change a et b l'une dans l'autre.

On peut trouver très-facilement la forme générale des fonctions qui n'ont que deux valeurs. Désignons par V une fonction quelconque qui n'a que deux valeurs distinctes, il est aisé de voir que le produit Vv n'aura aussi que deux valeurs. Soient, en effet, V et V_1 les deux valeurs de V, v et $-v$ étant celles de v; d'après ce qui a été établi précédemment, une substitution ne changera ni V ni v, si elle équivaut à un nombre pair de transpositions; au contraire, elle changera V en V_1 et v en $-v$, si elle équivaut à un nombre impair de transpositions; d'où il suit évidemment que la fonction Vv n'a que les deux valeurs Vv et $-V_1v$.

Si donc on fait

$$V + V_1 = A,$$

$$Vv - V_1 v = B,$$

A et B seront des fonctions symétriques (*voir* troisième leçon). De ces équations on déduit

$$V = \frac{A}{2} + \frac{B}{2v} = \frac{A}{2} + \frac{B}{2v^2}v;$$

mais $\frac{A}{2}$ et $\frac{B}{2v^2}$ sont des fonctions symétriques; on peut donc écrire plus simplement

$$V = A + Bv.$$

Telle est la forme générale des fonctions qui n'ont que deux valeurs; A et B désignent des fonctions symétriques, et v représente la fonction

$$(a-b)(a-c)\ldots(k-l),$$

dont les deux valeurs sont égales et de signes contraires.

VINGTIÈME LEÇON.

Théorème de M. Bertrand sur le nombre des valeurs que peut prendre une fonction de n lettres. — Forme générale des fonctions de n lettres qui ont n valeurs distinctes. — Examen des cas particuliers qui échappent à la démonstration précédente.

Théorème de M. Bertrand sur le nombre de valeurs que peut prendre une fonction de n lettres.

Postulatum. — Si n est un nombre entier > 7, il y a au moins un nombre premier p compris entre $n-2$ et $\frac{n}{2}$.

La démonstration du théorème de M. Bertrand, ainsi que celle du lemme qui va suivre, repose sur ce postulatum.

LEMME. — Soit

$$V = F(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres ayant moins de n valeurs. Si p désigne un nombre premier, compris entre $n-2$ et $\frac{n}{2}$, ou égal à $\frac{n}{2}$, et qu'avec les n lettres,

$$a, b, c, d, \ldots, k, l$$

on forme deux groupes, l'un de p lettres, l'autre de deux lettres, l'un au moins de ces deux groupes jouira de la propriété que la fonction V ne sera pas changée par une substitution circulaire effectuée sur les lettres qui le composent.

Soient a et b deux lettres quelconques parmi les n lettres données a, b, c, etc.; on formera, en les transposant, les deux arrangements ab et ba. Considérons aussi l'un des arrangements de p lettres prises parmi les $n-2$ qui restent,

effectuons sur les lettres de cet arrangement une substitution circulaire et répétons cette même substitution $p-1$ fois. On formera, de cette façon, p arrangements, et, en combinant chacun de ces p arrangements avec les deux des lettres a et b, on aura en tout $2p$ arrangements des $p+2$ lettres, auxquels correspondront $2p$ valeurs de la fonction V. Mais, par hypothèse, V a moins de n valeurs distinctes et $2p$ est au moins égal à n; donc, parmi les $2p$ valeurs de V, il y en a au moins deux qui sont égales entre elles. Cela posé, il convient de distinguer trois cas :

1°. Les deux valeurs égales de V correspondent à un même arrangement des p lettres et ne diffèrent que par l'ordre des deux lettres a et b. Alors on passe de l'une à l'autre des valeurs de V, par la transposition (a, b). Cette transposition ne change donc pas la valeur de V.

2°. Les deux valeurs égales de V correspondent à un même arrangement des deux lettres a et b, et à des arrangements différents des p autres lettres. Alors la fonction V n'est pas changée en effectuant plusieurs fois une même substitution circulaire sur ces p lettres; donc elle ne changera pas non plus en ne faisant qu'une seule fois cette substitution.

3°. Enfin, les deux valeurs de V correspondent à des arrangements qui diffèrent tant par l'ordre des deux lettres a et b que par celui des p autres lettres. Alors la fonction V n'est pas changée en effectuant un certain nombre r de fois, sur les p lettres, une même substitution circulaire, pourvu qu'on change en même temps les lettres a et b l'une dans l'autre. On pourra donc faire une seconde fois cette opération sans changer la valeur de V, mais alors a et b auront repris leurs places, et l'on aura seulement effectué sur les p lettres de l'autre groupe $2r$ fois une même substitution circulaire. D'où il suit, comme dans le second cas, qu'une substitution circulaire effectuée sur les p let-

tres ne changera pas la fonction. Et comme, après avoir fait plusieurs fois la substitution circulaire sur les p lettres, on peut, sans changer V, faire la transposition (a, b), cette transposition ne changera pas non plus la valeur de la fonction.

La proposition est donc démontrée.

Remarque. — La démonstration qui précède se fait, comme on voit, avec le même succès, que p soit compris entre $n-2$ et $\frac{n}{2}$, ou qu'il soit précisément égal à $\frac{n}{2}$. Mais si p est $>\frac{n}{2}$, on peut étendre un peu l'énoncé de la proposition, et dire :

Si une fonction de n lettres n'a pas plus de n valeurs, et si p désigne un nombre premier compris entre $n-2$ et $\frac{n}{2}$, en formant deux groupes, l'un de deux, l'autre de p lettres, il y aura au moins un de ces groupes qui jouira de la propriété que la fonction ne sera pas changée par une substitution circulaire effectuée sur les lettres qui le composent.

Ce nouvel énoncé ne serait pas exact si, entre $n-2$ et $\frac{n}{2}$, il n'y avait effectivement aucun nombre premier. Tel est le cas de $n=6$.

Théorème de M. Bertrand. — *Si une fonction de n lettres, non symétrique, a moins de n valeurs, elle ne peut en avoir plus de deux.*

Supposons que la fonction

$$V = F(a, b, c, d, \ldots, k, l)$$

des n lettres a, b, c, etc., ait moins de n valeurs. Cette fonction n'étant pas symétrique, il y aura au moins deux lettres a et b dont la transposition changera sa valeur. Désignons par p un nombre premier compris entre $n-2$

et $\frac{n}{2}$, ou égal à $\frac{n}{2}$, puis parmi les $n-2$ lettres

$$c,\ d,\ldots,\ k,\ l,$$

prenons-en p au hasard. D'après le lemme précédent, la fonction V ne sera pas changée par une substitution circulaire effectuée sur ces p lettres, puisqu'elle est changée par celle des deux lettres a et b, et que, parmi les deux groupes, l'un de deux, l'autre de p lettres, il y en a un sur lequel on peut effectuer une substitution circulaire sans changer la fonction.

Il suit de là que V, considérée comme fonction des $n-2$ lettres

$$c,\ d,\ldots,\ k,\ l,$$

n'est changée par aucune substitution circulaire de p lettres; par suite, elle ne l'est pas non plus par une substitution circulaire effectuée sur trois lettres quelconques; elle n'a donc au plus que deux valeurs (*voir* la leçon précédente).

Nous examinerons d'abord le cas où la fonction V est symétrique par rapport aux $n-2$ lettres $c, d,\ldots, k, l$, puis celui où elle a deux valeurs par les permutations de ces lettres.

1°. *V est symétrique par rapport aux $n-2$ lettres $c, d, \ldots, k, l$.*

Si V n'a pas précisément n valeurs, cette fonction changera par la transposition de l'une des lettres a et b avec l'une quelconque des $n-2$ autres; car autrement V serait symétrique par rapport à $n-1$ lettres, et aurait précisément n valeurs. On ne peut donc avoir

$$F(a, b, c, d, \ldots, k, l) = F(a, c, b, d, \ldots, k, l).$$

Il n'est pas possible non plus que V conserve la même valeur lorsque les deux lettres a et b sont changées en deux autres c et d, car on aurait alors

$$F(a, b, c, d, \ldots, k, l) = F(c, d, a, b, \ldots, k, l),$$

et le second membre serait symétrique par rapport à a et b, tandis que le premier ne l'est pas par hypothèse. Enfin l'égalité

$$F(a, b, c, d, \ldots, k, l) = F(b, c, a, d, \ldots, k, l)$$

est de même impossible; car le second membre est symétrique par rapport à a et d, tandis que le premier ne l'est pas.

D'où il suit que, si V n'a pas précisément n valeurs, cette fonction en aura autant qu'il y a d'arrangements de n lettres deux à deux, c'est-à-dire $n(n-1)$.

Comme, par hypothèse, la fonction V a moins de n valeurs, il est impossible qu'elle soit symétrique par rapport aux $n-2$ lettres, $c, d, \ldots, k, l$.

2°. *V a deux valeurs par les permutations des $n-2$ lettres $c, d, \ldots, k, l$.*

Je dis que, dans ce cas, la fonction V ne sera changée par aucune substitution circulaire effectuée sur p lettres quelconques prises parmi les n,

$$a, b, c, d, \ldots, k, l,$$

et, par suite, que cette fonction n'aura que deux valeurs distinctes par les permutations de ces n lettres.

Remarquons d'abord que V n'ayant que deux valeurs, par les permutations des $n-2$ lettres $c, d, \ldots, k, l$ change par la transposition de deux quelconques de ces lettres, et n'est pas changée par une substitution circulaire opérée sur p de ces $n-2$ lettres. Supposons maintenant qu'on prenne p lettres parmi les n lettres a, b, etc., et que parmi ces p lettres se trouvent a et b ou au moins l'une d'elles, il y aura au plus dans ce groupe $p-1$ lettres prises parmi $c, d, \ldots, k, l$; et comme p est $< n-2$, il restera au moins deux de ces dernières lettres qui ne feront pas partie du groupe de p lettres. Or la transposition de ces deux-là change la valeur de la fonction; donc, d'après le lemme

précédent, une substitution circulaire effectuée sur les p lettres ne la changera pas.

La fonction V n'étant changée par aucune substitution circulaire effectuée sur p lettres, ne le sera pas non plus par une substitution circulaire effectuée sur trois lettres, et, par conséquent, elle n'aura que deux valeurs, ainsi que nous l'avons vu dans la dernière leçon.

On voit donc que si entre $n-2$ et $\frac{n}{2}$ il y a un nombre premier, ou si $\frac{n}{2}$ est un nombre premier, une fonction de n lettres qui a moins de n valeurs ne peut en avoir que deux au plus.

En particulier, comme $\frac{6}{2}$ est un nombre premier, on a ce théorème démontré depuis longtemps par M. Cauchy :

Une fonction de six lettres, qui a moins de six valeurs, ne peut en avoir plus de deux.

Remarque. — La démonstration de M. Bertrand ne s'applique pas aux fonctions de quatre, de cinq et de sept lettres; mais, comme 5 et 7 sont des nombres premiers, le cas des fonctions de cinq lettres et celui des fonctions de sept lettres sont compris dans le théorème de M. Cauchy. Le seul cas des fonctions de quatre lettres fait exception. Il y a effectivement, comme nous l'avons vu dans les leçons précédentes, des fonctions de quatre lettres qui n'ont que trois valeurs distinctes.

Forme générale des fonctions de n lettres qui ont n valeurs distinctes.

Soit

$$V = F(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres $a, b, c, \ldots, k, l$, qui a précisément n valeurs, et supposons que la transposition (a, b) change la valeur de cette fonction; on fera voir, comme



précédemment, que la fonction V ne peut avoir que deux valeurs au plus par les permutations des $n-2$ lettres c, $d, \ldots, k, l$, pourvu qu'il existe un nombre premier compris entre $n-2$ et $\frac{n}{2}$; alors la fonction V doit être symétrique par rapport aux $n-2$ lettres $c, d, \ldots, k, l$, car, s'il en était autrement, on a vu qu'elle n'aurait que deux valeurs. Je dis même que la fonction V doit être symétrique par rapport à $n-1$ lettres, car autrement elle aurait $n(n-1)$ valeurs, comme nous l'avons fait voir tout à l'heure; d'où il résulte que, s'il existe un nombre premier compris entre $n-2$ et $\frac{n}{2}$, on a ce théorème :

THÉORÈME. — *Une fonction de n lettres qui a n valeurs est symétrique par rapport à n — 1 lettres.*

REMARQUE. — La démonstration, comme on le voit, ne s'applique pas aux fonctions de trois, de quatre, de cinq, de six et de sept lettres. Le théorème a été démontré par Abel, pour les fonctions de cinq lettres (*Œuvres complètes*, tome Ier, page 19), et il a lieu aussi pour les fonctions de trois, de quatre et de sept lettres; le seul cas des fonctions de six lettres fait exception; il y a, en effet, des fonctions de six lettres dont le nombre des valeurs distinctes est 6, et qui ne sont pas symétriques par rapport à cinq lettres (*voir* la Note VIII). Nous allons examiner ici les cas des fonctions de trois, de quatre, de cinq et de sept lettres.

Examen des cas particuliers qui échappent à la démonstration précédente.

Nous commencerons par établir le lemme général suivant :

Si une fonction d'un nombre n de lettres, supérieur à 3, n'a que deux valeurs distinctes par les permuta-

tions de $n-1$ lettres, elle a 2 ou $2n$ valeurs par les permutations de toutes les lettres.

Soit V une fonction des n lettres

$$a, b, c, d, \ldots, k, l,$$

qui a deux valeurs distinctes par les permutations des $n-1$ lettres

$$b, c, d, \ldots, k, l,$$

et supposons $n > 3$.

En désignant par ν le produit des différences de ces $n-1$ lettres deux à deux, en sorte qu'on ait

$$\nu = (b-c)(b-d)\ldots(k-l),$$

V aura la forme

$$V = A + B\nu,$$

A et B étant des fonctions des n lettres a, b, c, etc., symétriques, par rapport aux $n-1$ dernières.

Cela posé, je distinguerai deux cas, suivant que la fonction A est ou n'est pas symétrique par rapport aux n lettres.

1°. Si A est symétrique par rapport aux n lettres, V a précisément autant de valeurs que $B\nu$; mais le carré de $B\nu$ est symétrique par rapport aux $n-1$ lettres $b, c, d, \ldots, k, l$; donc ce carré a n valeurs, ou une valeur seulement s'il est symétrique par rapport à toutes les lettres. Par conséquent, $B\nu$ ou V a 2 ou $2n$ valeurs.

2°. Si A n'est symétrique que par rapport aux $n-1$ lettres $b, c, d, \ldots, k, l$, faisons les n transpositions

$$(a, a), \quad (a, b), \quad (a, c), \ldots, \quad (a, k), \quad (a, l),$$

et désignons par

$$A_1, \quad A_2, \ldots, \quad A_n$$

les valeurs qui en résultent pour A; par

$$B_1, \quad B_2, \ldots, \quad B_n$$

les valeurs correspondantes de B qui peuvent être égales entre elles; enfin par

$$v_1, \quad v_2, \ldots, \quad v_n$$

celles de v. On aura ces $2n$ valeurs de V, les seules que cette fonction puisse avoir :

$$\begin{aligned} &A_1 \pm B_1 v_1, \\ &A_2 \pm B_2 v_2, \\ &\ldots\ldots \ \ldots \\ &A_n \pm B_n v_n; \end{aligned}$$

et je dis que ces $2n$ valeurs de V sont différentes si n est > 3. En effet, si l'on avait, par exemple,

$$A_1 \pm B_1 v_1 = A_2 \pm B_2 v_2,$$

il en résulterait

$$A_1 - A_2 = \pm B_2 v_2 \mp B_1 v_1;$$

or le premier membre n'est pas nul, et il est symétrique par rapport aux $n-2$ lettres $c, d, \ldots, k, l$; B_1 et B_2 sont également symétriques par rapport à ces lettres, tandis que v_1 et v_2 changent de signe par la transposition de deux quelconques de ces $n-2$ lettres; l'égalité précédente est donc impossible si $n-2$ est au moins égal à 2, c'est-à-dire si n est > 3. La fonction V a donc $2n$ valeurs.

On peut déduire de cette proposition que :

Si une fonction d'un nombre n de lettres, supérieur à 3, a n valeurs, il est impossible que le nombre des valeurs que prend cette fonction par les permutations de $n-1$ lettres soit égal à 2.

Cela posé, je dis que pour chacune des quatre valeurs de n,

$$n = 3, \quad n = 4, \quad n = 5, \quad n = 7,$$

on a ce théorème :

Une fonction de n lettres qui a n valeurs distinctes est symétrique par rapport à $n-1$ lettres.

1°. *Cas des fonctions de trois lettres.* — Soit V une fonction des trois lettres

$$a, b, c,$$

qui a trois valeurs. Si V n'est pas symétrique par rapport à a et b, elle aura deux valeurs V_1 et V_2 par les permutations de ces lettres; nommons V_3 la troisième valeur de V. On a

$$V_3 = (V_1 + V_2 + V_3) - (V_1 + V_2);$$

or, ainsi que nous l'avons montré précédemment (troisième leçon), la fonction

$$V_1 + V_2 + V_3$$

est symétrique par rapport aux lettres a, b, c. Pareillement,

$$V_1 + V_2$$

est symétrique par rapport à a et b; donc V_3 est symétrique par rapport à a et b; donc enfin V est symétrique par rapport à deux lettres.

2°. *Cas des fonctions de quatre lettres.* — Soit V une fonction de quatre lettres

$$a, b, c, d,$$

qui a quatre valeurs. Le nombre des valeurs que prend V par les permutations des trois lettres a, b, c, est un diviseur du produit $1.2.3$; il est d'ailleurs au plus égal à 4. Si donc V n'est pas symétrique par rapport à a, b, c, elle a deux ou trois valeurs par les permutations de ces lettres. Le premier cas est impossible, d'après le lemme démontré plus haut; il faut donc que V ait trois valeurs V_1, V_2, V_3. Nommons V_4 la quatrième valeur de V; on a

$$V_4 = (V_1 + V_2 + V_3 + V_4) - (V_1 + V_2 + V_3),$$

d'où l'on peut conclure, comme plus haut, que V_4 est symétrique par rapport à a, b, c; donc V est symétrique par rapport à trois lettres.

3°. *Cas des fonctions de cinq lettres.* — Soit V une fonction de cinq lettres

$$a, b, c, d, e,$$

qui a cinq valeurs. Le nombre des valeurs que prend V par les permutations des quatre lettres a, b, c, d est un diviseur du produit 1.2.3.4, et, d'après l'hypothèse, ce nombre ne peut surpasser 5; ce sera donc l'un des nombres 1, 2, 3, 4. Si donc la fonction V n'est pas symétrique par rapport à a, b, c, d, elle a deux, trois ou quatre valeurs par les permutations de ces lettres. Le premier cas est impossible, d'après le lemme démontré plus haut; je dis que le second cas est aussi impossible. En effet, supposons que ce cas ait lieu; nommons V_1, V_2, V_3 les trois valeurs que prend V par les permutations des lettres a, b, c, d, et soient V_4, V_5 les deux autres valeurs de V; on a

$$V_4 + V_5 = (V_1 + V_2 + V_3 + V_4 + V_5) - (V_1 + V_2 + V_3),$$

$$V_4 V_5 = \frac{V_1 V_2 V_3 V_4 V_5}{V_1 V_2 V_3}:$$

on conclut de là que $V_4 + V_5$ et $V_4 V_5$ sont des fonctions symétriques de a, b, c, d; par suite, il en est de même de $(V_4 - V_5)^2$, et alors la fonction $V_4 - V_5$ a deux valeurs par les permutations de a, b, c, d (*). Posons

$$V_4 + V_5 = 2A, \quad V_4 - V_5 = 2B,$$

on aura

$$V_4 = A + B, \quad V_5 = A - B.$$

Il suit de là que V_4 a deux valeurs par les permutations de a, b, c, d; donc V a deux valeurs par les permutations

(*) On ne peut admettre que $V_4 - V_5$ soit symétrique par rapport à a, b, c, d; car alors V_4 et V_5 seraient symetriques par rapport à ces quatre lettres, par suite, V serait symétrique par rapport à quatre lettres, ce qui est contre l'hypothèse.

de quatre des cinq lettres a, b, c, d, e, ce que nous avons démontré impossible.

Il faut donc que V ait quatre valeurs V_1, V_2, V_3, V_4 par les permutations des quatre lettres a, b, c, d; nommons V_5 la cinquième valeur de V. L'égalité

$$V_5 = (V_1 + V_2 + V_3 + V_4 + V_5) - (V_1 + V_2 + V_3 + V_4)$$

montre que V_5 est symétrique par rapport à a, b, c, d; donc V est symétrique par rapport à quatre lettres.

4°. *Cas des fonctions de sept lettres.* — Soit V une fonction des sept lettres

$$a,\ b,\ c,\ d,\ e, f,\ g$$

qui a sept valeurs. Le nombre des valeurs que prend V par les permutations des six lettres

$$a,\ b,\ c,\ d,\ e, f,$$

est un diviseur du produit 1.2.3.4.5.6; et comme ce nombre est au plus égal à 7, ce sera nécessairement l'un des nombres 1, 2, 3, 4, 5 ou 6. D'ailleurs, une fonction de six lettres qui a moins de six valeurs n'en a au plus que deux; donc notre fonction V ne peut avoir que une, deux ou six valeurs par les permutations des six lettres a, b, c, d, e, f. Le second cas est impossible, d'après le lemme démontré plus haut; donc, si la fonction V n'est pas symétrique par rapport aux six lettres, elle a six valeurs par les permutations de ces lettres. Nommant alors V_1, V_2, V_3, V_4, V_5, V_6 ces six valeurs et V_7 la septième valeur de V, l'égalité

$$\begin{aligned} V_7 &= (V_1 + V_2 + V_3 + V_4 + V_5 + V_6 + V_7) \\ &\quad - (V_1 + V_2 + V_3 + V_4 + V_5 + V_6) \end{aligned}$$

montre que V_7 est symétrique par rapport à a, b, c, d, e, f, et, par suite, que V est symétrique par rapport à six lettres.

VINGT ET UNIÈME LEÇON.

Des fonctions algébriques. — Des fonctions entières. — Des fonctions rationnelles. — Classification des fonctions algébriques non rationnelles. — Forme générale des fonctions algébriques.

Des fonctions algébriques.

Les considérations développées dans la dix-huitième leçon et les suivantes donnent lieu de penser, sans toutefois le démontrer d'une manière rigoureuse, qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième. Abel est parvenu à démontrer cette impossibilité, par une méthode qui a été simplifiée ensuite par Wantzel dans quelques-unes de ses parties.

Résoudre une équation algébriquement, c'est former une fonction algébrique des coefficients qui, substituée à l'inconnue, satisfasse identiquement à l'équation ; la première chose à faire, pour reconnaître si une équation est soluble ou non algébriquement, est donc d'étudier la forme générale des fonctions algébriques. C'est cette étude que nous allons faire ici, et nous démontrerons, dans la prochaine leçon, l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Soient

$$x_1, \quad x_2, \quad x_3, \ldots, \quad x_k,$$

k quantités quelconques indépendantes, et v une fonction de ces quantités ; v sera une *fonction algébrique*, si on peut l'exprimer en x_1, x_2, x_3, etc., à l'aide des opérations suivantes, effectuées un nombre fini de fois : 1° l'addition

ou la soustraction; 2° la multiplication; 3° la division; 4° l'extraction des racines d'indices premiers. Nous ne comptons pas l'élévatiou aux puissances entières et l'extraction des racines de degrés composés, car ces opérations sont évidemment comprises dans les quatre que nous avons mentionnées.

Des fonctions entières.

Lorsque la fonction v peut se former par les deux premières des quatre opérations mentionnées ci-dessus, elle est dite rationnelle et entière ou simplement entière.

Désignons par

$$f(x_1, x_2, x_3, \ldots)$$

une fonction qui peut être exprimée par une somme d'un nombre limité de termes de la forme

$$A x_1^{m_1} x_2^{m_2} \ldots,$$

A désignant une constante, et m_1, m_2, etc., étant des exposants entiers et positifs. L'opération désignée par f fournit une fonction entière, conformément à la définition précédente; et l'on peut généralement considérer toutes les fonctions entières comme obtenues en répétant cette opération un nombre limité de fois. Soient v_1, v_2, etc., plusieurs fonctions de x_1, x_2, etc., de la même forme que f, la fonction

$$f(v_1, v_2, \ldots)$$

sera évidemment de la même forme. D'ailleurs $f(v_1, v_2, \ldots)$ est l'expression des fonctions obtenues en répétant deux fois l'opération $f(x_1, x_2, \ldots)$; d'où il suit qu'on trouvera toujours un résultat de même forme, en répétant cette même opération autant de fois que l'on voudra, et que toute fonction entière de x_1, x_2, etc., peut être exprimée par une somme de termes de la forme

$$A x_1^{m_1} x_2^{m_2} \ldots.$$

Des fonctions rationnelles.

Une fonction v des quantités x_1, x_2, x_3, etc., est dite rationnelle lorsqu'elle peut être exprimée par les trois premières des quatre opérations algébriques ci-dessus désignées.

Soient

$$f(x_1, x_2, x_3, \ldots), \qquad F(x_1, x_2, x_3, \ldots)$$

deux fonctions entières, le quotient de ces fonctions

$$\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)},$$

sera évidemment un cas particulier des fonctions rationnelles non entières, et l'on peut considérer toute fonction rationnelle comme obtenue en répétant plusieurs fois l'opération précédente; mais en désignant par v_1, v_2, etc., plusieurs fonctions de la forme $\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)}$, il est évident que la fonction

$$\frac{f(v_1, v_2, \ldots)}{F(v_1, v_2, \ldots)}$$

peut être réduite à la même forme; d'où il suit que toute fonction rationnelle se réduira à la forme

$$\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)},$$

f et F désignant des fonctions entières.

Classification des fonctions algébriques non rationnelles.

Soit

$$f(x_1, x_2, \ldots)$$

une fonction rationnelle quelconque; il est évident que

toute fonction algébrique s'obtiendra en combinant l'opération désignée par f avec l'opération désignée par $\sqrt[m]{\ }$, m étant un nombre premier. Si donc p_1, p_2 désignent des fonctions rationnelles de x_1, x_2, etc., n_1, n_2, etc., des nombres premiers, et qu'on fasse

$$p' = f\left(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots\right),$$

p' sera la forme des fonctions algébriques dans lesquelles l'opération désignée par $\sqrt[m]{\ }$ ne porte que sur des fonctions rationnelles. Nous appellerons, avec Abel, *fonctions algébriques du premier ordre* les fonctions de la forme p'.

Soient p'_1, p'_2, etc., des fonctions algébriques du premier ordre, n'_1, n'_2, etc., des nombres premiers; et posons

$$p'' = f\left(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots, \sqrt[n'_1]{p'_1}, \sqrt[n'_2]{p'_2}, \ldots\right),$$

p'' sera la forme générale des fonctions algébriques dans lesquelles l'opération désignée par $\sqrt[m]{\ }$ ne porte que sur des fonctions rationnelles ou sur des fonctions algébriques du premier ordre. Nous appellerons *fonctions algébriques du deuxième ordre* les fonctions de la forme p''.

De même si p''_1, p''_2, etc., désignent des fonctions algébriques du deuxième ordre, n''_1, n''_2, etc., des nombres premiers, et qu'on fasse

$$p''' = f\left(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \ldots, \sqrt[n'_1]{p'_1}, \ldots, \sqrt[n''_1]{p''_1}, \ldots\right),$$

p''' sera la forme des fonctions algébriques, où l'opération désignée par $\sqrt[m]{\ }$ ne porte que sur des fonctions rationnelles et sur des fonctions des deux premiers ordres. Les fonctions de la forme p''' seront les fonctions algébriques du troisième ordre.

En continuant ainsi, on formera des fonctions algé-

briques du quatrième, cinquième, etc., $\mu^{ième}$ ordre, et il est évident que l'expression générale des fonctions du $\mu^{ième}$ ordre sera l'expression générale des fonctions algébriques.

Il suit de là qu'en désignant par v une fonction algébrique du $\mu^{ième}$ ordre, v aura la forme

$$v = f\left(r_1, r_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots\right),$$

où f désigne toujours une fonction rationnelle, p_1, p_2, etc., des fonctions de l'ordre $\mu - 1$, n_1, n_2, etc., des nombres premiers, et r_1, r_2, etc., des fonctions de l'ordre $\mu - 1$ ou d'ordres moins élevés.

On peut évidemment supposer qu'aucun des radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, etc., ne soit exprimable rationnellement en fonction des autres radicaux et des quantités r_1, r_2, etc. Si, en effet, $\sqrt[n_1]{p_1}$ était dans ce cas, en portant sa valeur dans l'expression de v, on aurait une valeur de v

$$v = f\left(r_1, r_2, \ldots, \sqrt[n_2]{p_2}, \ldots\right)$$

de la même forme que la précédente, mais plus simple, puisqu'elle contiendrait le radical $\sqrt[n_1]{p_1}$ de moins. Si de même l'un des radicaux qui restent pouvait s'exprimer en fonction rationnelle des autres radicaux et des quantités r_1, r_2, etc., on pourrait chasser ce radical de l'expression de v, qui conserverait d'ailleurs la même forme; et si l'on pouvait continuer ainsi jusqu'à ce qu'on eût éliminé tous les radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, etc., la fonction v serait réduite à l'ordre $\mu - 1$.

Si donc la fonction v est effectivement du $\mu^{ième}$ ordre, on peut supposer que les radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, etc., aient

été réduits au plus petit nombre possible, et qu'il soit impossible d'exprimer l'un de ces radicaux en fonction rationnelle des autres et de fonctions algébriques d'ordre inférieur. Et si m désigne alors le nombre de ces radicaux qui affectent des fonctions algébriques d'ordre $\mu - 1$, nous dirons que la fonction v d'ordre μ est du *degré m*.

D'après cette définition, une fonction d'ordre μ et de degré zéro n'est autre qu'une fonction d'ordre $\mu - 1$, et une fonction d'ordre zéro est une fonction rationnelle.

Il résulte de là que si v désigne une fonction algébrique d'ordre μ et de degré m, on aura généralement

$$v = f(r_1, r_2, \ldots, \sqrt[n]{p}),$$

f désignant une fonction rationnelle, p une fonction algébrique d'ordre $\mu - 1$, n un nombre premier, et r_1, r_2, etc., des fonctions d'ordre μ, mais de degré $m - 1$. En outre, d'après ce qui précède, on peut toujours supposer qu'il soit impossible d'exprimer $\sqrt[n]{p}$ en fonction rationnelle de r_1, r_2, etc.

Forme générale des fonctions algébriques.

Dans l'expression précédente de v, f désigne une fonction rationnelle des quantités r_1, r_2, etc., et $\sqrt[n]{p}$, mais toute fonction rationnelle de plusieurs quantités peut être représentée par le quotient de deux fonctions entières; nous pouvons donc poser

$$v = \frac{\varphi(r_1, r_2, \ldots, \sqrt[n]{p})}{\psi(r_1, r_2, \ldots, \sqrt[n]{p})},$$

φ et ψ désignant des fonctions entières, et si l'on ordonne φ et ψ par rapport aux puissances de $\sqrt[n]{p}$ ou $p^{\frac{1}{n}}$, on aura

pour ν une valeur de la forme

$$\nu = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} + \ldots + s_\nu p^{\frac{\nu}{n}}}{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} + \ldots + t_{\nu'} p^{\frac{\nu'}{n}}} = \frac{S}{T},$$

où $s_0, s_1, \ldots, s_\nu$ et $t_0, t_1, \ldots, t_{\nu'}$, sont des fonctions entières de r_1, r_2, etc.

Soit α une racine imaginaire de l'équation

$$\alpha^n = 1;$$

désignons par

$$T_1, T_2, \ldots, T_{n-1}$$

les $n-1$ valeurs qu'on obtient en remplaçant dans T, $p^{\frac{1}{n}}$ successivement par

$$\alpha p^{\frac{1}{n}}, \quad \alpha^2 p^{\frac{1}{n}}, \quad \alpha^3 p^{\frac{1}{n}}, \ldots, \alpha^{n-1} p^{\frac{1}{n}},$$

et multiplions par $T_1 T_2 \ldots T_{n-1}$ les deux termes de la valeur de ν, on aura

$$\nu = \frac{S T_1 T_2 \ldots T_{n-1}}{T T_1 T_2 \ldots T_{n-1}}.$$

Le produit $T_1 T_2 \ldots T_{n-1}$ peut évidemment s'exprimer en fonction entière de p et des quantités r_1, r_2, etc.; il est donc une fonction algébrique d'ordre μ et de degré $m-1$ au plus, que nous désignerons par u. Pareillement, le produit $S T_1 T_2 \ldots T_{n-1}$ est une fonction entière de r_1, r_2, etc., et $\sqrt[n]{p}$; nous représenterons sa valeur par

$$u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \ldots + u_i p^{\frac{i}{n}},$$

et l'on aura

$$\nu = \frac{u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \ldots + u_i p^{\frac{i}{n}}}{u},$$

ou simplement

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_i p^{\frac{i}{n}},$$

en mettant q_0, q_1, etc., au lieu de $\frac{u_0}{u}$, $\frac{u_1}{u}$, etc.; q_0, q_1, etc., désignent ici des fonctions rationnelles de r_1, r_2, etc., et p.

On peut chasser de l'expression précédente de v les puissances de $p^{\frac{1}{n}}$ supérieures à la $(n-1)^{ième}$. Si, en effet, j désigne un nombre qui, divisé par n, donne le quotient g et le reste h, on a

$$p^{\frac{j}{n}} = p^g . p^{\frac{h}{n}},$$

et, en se servant de cette formule, on pourra mettre v sous la forme

$$(1) \qquad v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

q_0, q_1, q_2, ..., q_{n-1} étant toujours des fonctions rationnelles de p, r_1, r_2, etc., et, par conséquent, des fonctions algébriques d'ordre μ et de degré $m-1$ au plus, telles, en outre, qu'il soit impossible d'exprimer rationnellement $p^{\frac{1}{n}}$ en fonction des quantités dont elles dépendent.

Dans l'expression (1) de v, on peut supposer

$$q_1 = 1.$$

Pour le démontrer, supposons d'abord que q_1 ne soit pas nul, et posons

$$p_1 = p q_1^n;$$

d'où

$$p = \frac{p_1}{q_1^n} \quad \text{et} \quad p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1};$$

l'expression de v devient

$$v = q_0 + p_1^{\frac{1}{n}} + \frac{q_2}{q_1^2} p_1^{\frac{2}{n}} + \ldots + \frac{q_{n-1}}{q_1^{n-1}} p_1^{\frac{n-1}{n}},$$

ou plus simplement

$$(2)\qquad v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

en écrivant p au lieu de p_1; q_2, q_3, etc., au lieu de $\frac{q_2}{q_1^2}$, $\frac{q_3}{q_1^3}$, etc.

Dans cette nouvelle expression (2) de v qui se déduit de (1) en faisant $q_1 = 1$, les quantités q_0, q_2, etc., désignent toujours des fonctions algébriques d'ordre μ et de degré $m - 1$.

Supposons maintenant que dans l'expression (1) de v on ait $q_1 = 0$; désignons par q_k l'une des quantités q_2, q_3, etc., qui n'est pas nulle, et posons

$$p_1 = q_k^n p^k,$$

d'où

$$p_1^{\frac{\alpha}{n}} = q_k^{\alpha} p^{\frac{k\alpha}{n}}.$$

n étant premier et k moindre que n, on peut toujours trouver deux entiers α et 6 tels, que

$$k\alpha - n6 = \lambda,$$

λ étant un nombre entier quelconque donné; alors on aura

$$p_1^{\frac{\alpha}{n}} = q_k^{\alpha} p^{6} p^{\frac{\lambda}{n}},$$

d'où

$$p^{\frac{\lambda}{n}} = q_k^{-\alpha} p^{-6} p_1^{\frac{\alpha}{n}}.$$

On a, en particulier et par hypothèse,

$$p^{\frac{k}{n}} = \frac{p_1^{\frac{1}{n}}}{q_k}:$$

à l'aide des deux formules précédentes, on substituera aux puissances de $p^{\frac{1}{n}}$ dans la valeur (1) de ν, celles de $p_1^{\frac{1}{n}}$, et, après cette substitution, il est évident que la forme de ν n'aura pas changé, mais que le coefficient de $p_1^{\frac{1}{n}}$ sera l'unité; car, dans l'expression primitive de ν, $p^{\frac{k}{n}}$ a pour coefficient q_k.

Conclusion. — *Il résulte de ce qui précède que toute fonction algébrique d'ordre* μ *et de degré* m *peut être mise sous la forme*

$$\nu = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

où n *est un nombre premier,* q_0, q_2, *etc., des fonctions algébriques d'ordre* μ, *mais de degré* $m-1$, *et* p *une fonction d'ordre* $\mu - 1$, *dont la racine* $n^{\text{ième}}$ *ne peut être exprimée rationnellement par les quantités* q_0, q_2, *etc.*

VINGT-DEUXIÈME LEÇON.

Propriétés des fonctions algébriques qui satisfont à une équation donnée. — Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Propriétés des fonctions algébriques qui satisfont à une équation donnée.

Si l'on considère un polynôme entier et rationnel

$$x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots,$$

dont les coefficients a_1, a_2,... soient des nombres commensurables donnés, tout diviseur de ce polynôme dont les coefficients sont commensurables est dit un *diviseur commensurable*.

Plus généralement, si les coefficients a_1, a_2,... du polynôme sont des fonctions rationnelles de quantités quelconques, qu'on regarde comme connues, tout diviseur de ce polynôme qui a pour coefficients des fonctions rationnelles des quantités connues, est appelé un *diviseur commensurable*.

On nomme, dans tous les cas, *équation irréductible* toute équation dont le premier membre n'admet aucun diviseur commensurable.

Dans le cas de l'équation générale de degré quelconque, dont les coefficients sont indéterminés, les quantités connues ne sont autres que les coefficients eux-mêmes; l'équation est nécessairement irréductible.

Cela posé, soit une équation de degré m

$$(1) \qquad x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_{m-1} x + a_m = 0,$$

dont les coefficients sont considérés comme des fonctions

rationnelles de quantités connues, et supposons qu'elle soit résoluble algébriquement.

D'après la classification des fonctions algébriques établie dans la leçon précédente, si la racine x est une fonction algébrique d'ordre μ des quantités connues, on pourra poser

$$(2) \qquad x = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1}^{\frac{n-1}{n}}.$$

n est un nombre premier; p désigne une fonction d'ordre $\mu - 1$; q_0, q_2, etc., peuvent être de l'ordre μ, mais sont d'un degré moindre que celui de x. Enfin, on peut supposer qu'il soit impossible d'exprimer $p^{\frac{1}{n}}$ en fonction rationnelle de p, q_0, q_1, etc.

En substituant cette expression (2) de x dans l'équation (1), on aura un résultat qui pourra évidemment se réduire à la forme

$$(3) \qquad r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \ldots + r_{n-1} p^{\frac{n-1}{n}} = 0,$$

où $r_0, r_1, r_2, \ldots, r_{n-1}$ désignent des fonctions rationnelles des quantités $p, q_0, q_2, \ldots, q_{n-1}$. Or je dis que l'équation (3) exige que l'on ait en même temps

$$r_0 = 0, \quad r_1 = 0, \quad r_2 = 0, \ldots, \quad r_{n-1} = 0.$$

En effet, dans le cas contraire, les deux équations

$$z^n - p = 0,$$
$$r_0 + r_1 z + r_2 z^2 + \ldots + r_{n-1} z^{n-1} = 0$$

auraient une ou plusieurs racines communes. Soit k le nombre de ces racines, on pourrait former une équation de degré k ayant pour racines ces k racines communes, et pour coefficients des fonctions rationnelles de p, q_0, $q_1, \ldots, q_{n-1}$. Soit

$$s_0 + s_1 z + s_2 z^2 + \ldots + s_k z^k = 0$$

cette équation, et désignons par

$$t_0 + t_1 z + t_2 z^2 + \ldots + t_i z^i$$

un diviseur irréductible de son premier membre, dont les coefficients $t_0, t_1, \ldots, t_i$ soient des fonctions rationnelles de $p, q_0, q_2, \ldots, q_{n-1}$. L'équation

$$(4)\qquad t_0 + t_1 z + t_2 z^2 + \ldots + t_i z^i = 0$$

a toutes ses racines communes avec

$$(5)\qquad z^n - p = 0;$$

d'ailleurs son degré i est au moins égal à 2, car, autrement, on pourrait exprimer z ou $p^{\frac{1}{n}}$ en fonction rationnelle de $p, q_0, q_2, \ldots, q_{n-1}$. Si donc z désigne une racine quelconque de l'équation (4), cette équation aura au moins une autre racine de la forme αz, α étant une racine de l'équation

$$\alpha^n = 1;$$

l'équation (4) aura donc une racine commune avec

$$(6)\qquad t_0 + t_1 \alpha z + t_2 \alpha^2 z^2 + \ldots + t_i \alpha^i z^i = 0,$$

et, par conséquent, avec l'équation

$$(7)\quad (1 - \alpha^i) t_0 + (\alpha - \alpha^i) t_1 z + \ldots + (\alpha^{i-1} - \alpha^i) t_{i-1} z^{i-1} = 0,$$

que l'on obtient en retranchant de l'équation (6) l'équation (4) multipliée par α^i. Mais l'équation (4) est supposée irréductible; il est donc impossible qu'elle ait une racine commune avec l'équation (7), qui est d'un degré inférieur au sien. D'où il suit qu'on a nécessairement

$$r_0 = 0, \quad r_1 = 0, \ldots, \quad r_{n-1} = 0.$$

Les équations précédentes ayant lieu, l'expression (2) de x satisfera encore à la proposée (1), en remplaçant $p^{\frac{1}{n}}$

par chacune des n valeurs

$$p^{\frac{1}{n}},\quad \alpha p^{\frac{1}{n}},\quad 6 p^{\frac{1}{n}},\ldots,\quad \omega p^{\frac{1}{n}},$$

où $1, \alpha, 6, \ldots, \omega$ désignent les racines $n^{\text{ièmes}}$ de l'unité. On aura ainsi n racines de l'équation (1), que nous représenterons par

$$x_1,\quad x_2,\ldots,\quad x_n,$$

et dont les valeurs seront

$$(8)\quad \begin{cases} x_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots\ldots + q_{n-1} p^{\frac{n-1}{n}}, \\ x_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \ldots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ x_3 = q_0 + 6 p^{\frac{1}{n}} + 6^2 q_2 p^{\frac{2}{n}} + \ldots + 6^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = q_0 + \omega p^{\frac{1}{n}} + \omega^2 q_2 p^{\frac{2}{n}} + \ldots + \omega^{n-1} q_{n-1} p^{\frac{n-1}{n}}; \end{cases}$$

on voit que ces racines sont différentes, car, si deux d'entre elles étaient égales, on aurait une équation de cette forme,

$$(\alpha - 6) q_0 + (\alpha - 6) p^{\frac{1}{n}} + (\alpha^2 - 6^2) q_2 p^{\frac{2}{n}} + \ldots = 0,$$

qui conduirait aux équations contradictoires

$$(\alpha - 6) q_0 = 0,\quad (\alpha - 6) = 0, \ldots.$$

Au surplus, cette remarque n'est pas indispensable pour ce qui va suivre.

En ajoutant les équations (8), en les ajoutant ensuite après les avoir respectivement multipliées par

$$1,\quad \alpha^{n-1},\quad 6^{n-1},\ldots,\quad \omega^{n-1},$$

puis par

$$1,\quad \alpha^{n-2},\quad 6^{n-2},\ldots,\quad \omega^{n-2},$$

puis, etc.,

on obtient les suivantes :

$$q_0 = \frac{1}{n}(x_1 + x_2 + x_3 + \ldots\ldots\ldots + x_n),$$

$$p^{\frac{1}{n}} = \frac{1}{n}(x_1 + \alpha^{n-1} x_2 + \ldots\ldots + \omega^{n-1} x_n),$$

$$q_2 p^{\frac{2}{n}} = \frac{1}{n}(x_1 + \alpha^{n-2} x_2 + \ldots\ldots + \omega^{n-2} x_n),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$q_{n-1} p^{\frac{n-1}{n}} = \frac{1}{n}(x_1 + \alpha x_2 + \ldots\ldots\ldots\ldots + \omega x_n).$$

Il résulte de là que les quantités

$$p^{\frac{1}{n}},\quad q_0,\quad q_2,\ldots,\quad q_{n-1}$$

sont des fonctions rationnelles des racines de l'équation (1). On a, en effet, généralement

$$q_\rho = n^{\rho-1} \frac{x_1 + \alpha^{n-\rho} x_2 + \beta^{n-\rho} x_3 + \ldots + \omega^{n-\rho} x_n}{(x_1 + \alpha^{n-1} x_2 + \beta^{n-1} x_3 + \ldots + \omega^{n-1} x_n)^\rho}.$$

Désignons maintenant par y l'une quelconque des quantités $p^{\frac{1}{n}}$, q_0, q_2, ..., q^{n-1}, et soit

(9) $$y = s_0 + v^{\frac{1}{r}} + s_2 v^{\frac{2}{r}} + \ldots + s_{r-1} v^{\frac{r-1}{r}},$$

s_0, s_2, etc., étant des fonctions qui peuvent être du même ordre que y, mais qui sont de degré inférieur. On a, par ce qui précède,

$$y = \varphi(x_1, x_2, \ldots, x_m),$$

φ désignant une fonction rationnelle, et $x_1, x_2, \ldots, x_m$ les m racines de l'équation (1), lesquelles peuvent ne pas entrer toutes dans la fonction φ. Soit m' le nombre de valeurs que prend la fonction φ quand on y permute les

racines x_1, x_2, etc.; on pourra former une équation du degré m' dont les coefficients seront exprimés rationnellement par ceux de l'équation (1), et dont les racines

$$y_1, \quad y_2, \ldots, \quad y_{m'}$$

seront les m' valeurs de la fonction φ. Et comme la valeur (9) de y doit satisfaire à cette équation, on en conclura, comme précédemment, que les quantités

$$v, \quad s_0, \quad s_2, \ldots, \quad s_{p-1}$$

sont des fonctions rationnelles de $y_1, y_2, \ldots, y_{m'}$, et, par conséquent, aussi de $x_1, x_2, \ldots, x_m$.

Comme on peut continuer indéfiniment ce raisonnement, on conclut de ce qui précède, que

Si une équation est résoluble algébriquement, on peut donner à la racine une forme telle, que toutes les fonctions algébriques dont elle est composée soient des fonctions rationnelles des racines de l'équation proposée.

Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Les propriétés des racines d'une équation résoluble algébriquement, que nous venons de démontrer, ont lieu dans tous les cas, soit qu'il s'agisse d'une équation dont les coefficients ont des valeurs déterminées, soit que l'on considère ces coefficients comme indéterminés, et, par suite, les racines de l'équation comme étant des quantités quelconques, n'ayant entre elles aucune dépendance.

Nous plaçant maintenant à ce dernier point de vue, nous allons démontrer qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Ce théorème a été démontré, pour la première fois, par Abel; mais je présenterai ici la démonstration très-remarquable de Wantzel. On verra, dans cette reproduction exacte, un hommage mérité à la mémoire d'un géomètre que la mort a frappé dans toute la force de son talent. Je supprimerai pourtant quelques détails, inutiles ici, après les développements que j'ai donnés sur le nombre de valeurs qu'une fonction peut acquérir (*).

Soit

$$f(x) = 0$$

une équation de degré m dont les coefficients sont indéterminés, et désignons par

$$x_1, \ x_2, \ldots, \ x_m$$

ses m racines, que nous supposons exprimables algébriquement en fonction des coefficients.

« Si l'équation $f(x) = 0$ est satisfaite par la valeur x_1 » de x, quels que soient ses coefficients, on doit reproduire identiquement x_1, en substituant dans son expression la fonction rationnelle correspondante à chaque radical, puisque les racines de l'équation sont alors entièrement arbitraires. De même, toute relation entre les racines devra être identique, et ne cessera pas d'exister, si l'on y remplace ces racines les unes par les autres, d'une manière quelconque.

» Désignons par y le premier radical qui entre dans la valeur de x_1, en suivant l'ordre du calcul, et soit

$$y^n = p;$$

» p dépendra immédiatement des coefficients de $f(x)=0$, » et s'exprimera par une fonction symétrique des racines

(*) Les guillemets indiquent tout ce qui est emprunté littéralement au Mémoire de Wantzel.

» $F(x_1, x_2, x_3, \ldots)$; y sera une fonction rationnelle
» $\varphi(x_1, x_2, x_3, \ldots)$ des mêmes racines.

» Comme la fonction φ n'est pas symétrique, sans quoi
» la racine $n^{ième}$ de p s'extrairait exactement, elle doit
» changer lorsqu'on permute deux racines, x_1, x_2, par
» exemple; mais la relation

$$\varphi^n = F$$

» sera toujours satisfaite. D'ailleurs, la fonction F étant
» invariable par cette permutation, les valeurs de φ sont
» des racines de l'équation $y^n = F$, et l'on a

$$\varphi(x_2, x_1, x_3, \ldots) = \alpha\varphi(x_1, x_2, x_3, \ldots),$$

» α étant une racine $n^{ième}$ de l'unité.

» Si l'on remplace de part et d'autre x_1 par x_2, et réci-
» proquement, il vient

$$\varphi(x_1, x_2, x_3, \ldots) = \alpha\varphi(x_2, x_1, x_3, \ldots);$$

» d'où, en multipliant par ordre,

$$\alpha^2 = 1.$$

» Ce résultat prouve que le nombre n, supposé pre-
» mier, est nécessairement égal à 2; *donc le premier*
» *radical qui se présente dans la valeur de l'inconnue*
» *doit être du second degré*. C'est ce qui arrive, en effet,
» pour les équations qu'on sait résoudre. »

La fonction φ n'ayant que deux valeurs, change par une transposition quelconque, et ne sera pas changée (*voir* dix-neuvième leçon) par une permutation circulaire de trois ou de cinq lettres, car ces permutations équivalent à un nombre pair de transpositions.

Continuons la série des opérations indiquées pour former la valeur x_1 de x.

« On combinera le premier radical avec les coefficients

» de $f(x)=0$, ou la fonction φ avec des fonctions symé-
» triques des racines, à l'aide des premières opérations
» de l'algèbre, et l'on obtiendra ainsi une fonction des
» racines susceptible de deux valeurs, et, par conséquent,
» invariable par les permutations circulaires de trois
» lettres. Les radicaux subséquents pourront donner en-
» core des fonctions du même genre, s'ils sont du second
» degré. Supposons qu'on soit arrivé à un radical pour
» lequel la fonction rationnelle équivalente ne soit pas
» invariable par ces permutations. Désignons-le toujours
» par

$$y=\varphi(x_1, x_2, x_3, \ldots);$$

» dans l'équation

$$y^n=p$$

» nous ferons encore

$$p=\mathrm{F}(x_1, x_2, x_3, \ldots);$$

» cette fonction ne sera plus symétrique, mais seulement
» invariable par les permutations circulaires de trois
» lettres. Si l'on remplace

$$x_1,\ x_2,\ x_3$$

» par

$$x_2,\ x_3,\ x_1$$

» dans φ, la relation

$$\varphi^n=\mathrm{F}$$

» subsistera toujours; et, puisque F ne change pas par
» cette substitution, il viendra

$$\varphi(x_2, x_3, x_1, x_4, \ldots)=\alpha\varphi(x_1, x_2, x_3, x_4, \ldots),$$

» α désignant une racine $n^{\text{ième}}$ de l'unité. »

En faisant dans cette équation la substitution circulaire

$$\begin{pmatrix} x_1, & x_2, & x_3 \\ x_2, & x_3, & x_1 \end{pmatrix},$$

et répétant une seconde fois cette substitution, on aura

$$\varphi(x_3, x_1, x_2, x_4, \ldots) = \alpha\varphi(x_2, x_3, x_1, x_4, \ldots),$$
$$\varphi(x_1, x_2, x_3, x_4, \ldots) = \alpha\varphi(x_3, x_1, x_2, x_4, \ldots),$$

et, en multipliant les trois équations précédentes, « on
» conclura

$$\alpha^3 = 1.$$

» Ainsi, n sera égal à 3.

» Si le nombre des quantités x_1, x_2, x_3, x_4, etc., est
» supérieur à quatre, ou si l'équation $f(x) = 0$ est d'un
» degré plus élevé que le quatrième, on pourra effectuer
» dans φ une substitution circulaire de cinq lettres, en
» remplaçant

$$x_1,\ x_2,\ x_3,\ x_4,\ x_5$$

» par

$$x_2,\ x_3,\ x_4,\ x_5,\ x_1;$$

» la fonction F ne changera pas, et l'on aura

$$\varphi(x_2, x_3, x_4, x_5, x_1, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

» puis, en répétant de part et d'autre la même substi-
» tution,

$$\varphi(x_3, x_4, x_5, x_1, x_2, \ldots) = \alpha\varphi(x_2, x_3, x_4, x_5, x_1, \ldots),$$

....

» Par la multiplication, on obtient

$$\alpha^5 = 1,$$

» ce qui entraîne

$$\alpha = 1,$$

» puisque α est une racine cubique de l'unité. Ainsi la
» fonction φ est invariable par les permutations circu-
» laires de cinq lettres. » Donc, d'après un théorème

démontré dans la dix-neuvième leçon, la fonction φ est aussi invariable par les permutations circulaires de trois lettres.

« Ainsi, *tous les radicaux renfermés dans la racine* » *d'une équation générale de degré supérieur au qua-* » *trième devraient être égaux à des fonctions ration-* » *nelles des racines invariables par les permutations* » *circulaires de trois racines*. En substituant ces fonctions » dans l'expression de x_1, on arrive à une égalité de la » forme

$$x_1 = \psi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

» qui doit être identique; ce qui est impossible, puisque » le second membre reste invariable quand on remplace » x_1, x_2, x_3 par x_2, x_3, x_1, tandis que le premier change » évidemment.

» Donc, il est impossible de résoudre par radicaux » une équation générale du cinquième degré ou de degré » supérieur.

» La démonstration précédente fait voir en même temps » que, pour les équations du troisième et du quatrième » degré, le premier radical, dans l'ordre des opérations, » doit être un radical carré, et le second un radical » cubique. Ces circonstances se présentent, en effet, dans » les formules données par Lagrange et les autres géo- » mètres. »

VINGT-TROISIÈME LEÇON.

Des nombres congrus ou équivalents.—Theorème de Fermat.—Théorème de Wilson. — Des congruences en général. — Limite du nombre des racines d'une congruence suivant un module premier. — Détermination du nombre de racines d'une congruence. — Nouvelle démonstration du théorème de Wilson.

Des nombres congrus ou équivalents.

Si la différence de deux nombres entiers a et b, positifs ou négatifs, est divisible par un troisième nombre positif p, a et b sont dits *congrus* ou *équivalents* par rapport à p; le diviseur p est appelé le *module; a* et b sont *résidus l'un de l'autre* suivant le module p.

Pour exprimer que a et b sont congrus suivant le module p, il suffit d'écrire

$$a = b + \text{un multiple de } p;$$

mais nous adopterons la notation plus commode de M. Gauss, et nous écrirons

$$a \equiv b \pmod{p}.$$

Si r désigne le reste de la division de a par p, on a

$$a \equiv r \pmod{p},$$

et le reste r est, si l'on veut, compris entre o et p, ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$; d'où il suit que tout nombre a un résidu inférieur en valeur absolue à la moitié du module. On le nomme *résidu minimum;* mais, si l'on ne veut con-

sidérer que les résidus positifs, les limites seront o et p, et le résidu minimum pourra surpasser $\frac{p}{2}$.

Le principal avantage de la notation de M. Gauss, pour représenter les congruences, consiste en ce qu'elle rappelle la grande analogie qui existe entre les congruences et les égalités, sans qu'il y ait pourtant de confusion à craindre. Nous allons faire voir que la plupart des transformations que l'on peut faire subir aux égalités peuvent être appliquées aux congruences.

Addition et soustraction. — Si l'on a

$$a \equiv b \pmod{p},$$
$$a' \equiv b' \pmod{p},$$

on aura aussi

$$a \pm a' \equiv b \pm b' \pmod{p}.$$

Les congruences proposées expriment, en effet, que

$$a = b + \text{un multiple de } p,$$
$$a' = b' + \text{un multiple de } p;$$

donc

$$a \pm a' = b \pm b' + \text{un multiple de } p,$$

ou

$$a \pm a' \equiv b \pm b' \pmod{p}.$$

Ce qu'il fallait démontrer.

Multiplication. — On peut multiplier une congruence par un nombre quelconque. Car soit

$$a \equiv b \pmod{p},$$

c'est-à-dire

$$a = b + \text{un multiple de } p,$$

on aura aussi, quel que soit l'entier m,

$$ma = mb + \text{un multiple de } p,$$

ou

$$ma \equiv mb \pmod{p}.$$

On peut aussi multiplier entre elles plusieurs con-

gruences de même module. Soient, en effet, deux congruences

$$a \equiv b \quad (\text{mod. } p),$$
$$a' \equiv b' \quad (\text{mod. } p),$$

ou

$$a = b + \text{un multiple de } p,$$
$$a' = b' + \text{un multiple de } p.$$

On aura, en multipliant,

$$aa' = bb' + \text{un multiple de } p,$$

ou

$$aa' \equiv bb' \quad (\text{mod. } p).$$

Ce qu'il fallait démontrer.

On voit généralement que, si l'on a

$$\left.\begin{cases} a \equiv b, \\ a' \equiv b', \\ \dots\dots\dots \\ a^{(m)} = b^{(m)}, \end{cases}\right. \quad (\text{mod. } p),$$

on aura aussi

$$aa' \dots a^{(m)} \equiv bb' \dots b^{(m)}.$$

Élévation aux puissances. — On peut élever à une même puissance les deux membres d'une congruence. Cela résulte immédiatement de ce que nous venons de dire au sujet de la multiplication. Si donc on a

$$a \equiv b \quad (\text{mod. } p),$$

on aura aussi

$$a^m \equiv b^m \quad (\text{mod. } p).$$

Corollaire. — Soit

$$f(x) = \mathrm{A}x^m + \mathrm{B}x^n + \dots$$

une fonction entière et rationnelle de x, dont les coefficients A, B, etc., soient des nombres entiers; si l'on a

$$a \equiv b \quad (\text{mod. } p),$$

on aura aussi

$$f(a) \equiv f(b) \pmod{p}.$$

Division. — On peut diviser une congruence par un nombre quelconque premier avec le module.

Soient, en effet, la congruence

$$ma \equiv mb \pmod{p},$$

ou

$$ma = mb + p \times q,$$

on aura, en divisant par m,

$$a = b + \frac{p \times q}{m},$$

et, si l'on suppose m premier avec p, q devra être divisible par m, et l'on aura

$$a = b + \text{un multiple de } p,$$

ou

$$a \equiv b \pmod{p}.$$

Ce qu'il fallait démontrer.

On peut aussi diviser une congruence par une autre, pourvu que les membres de la seconde soient premiers avec le module. Soient, en effet, les deux congruences

(1) $$aa' \equiv bb' \pmod{p},$$

(2) $$a \equiv b \pmod{p}.$$

Désignons par r le résidu minimum de la différence $a' - b'$, on aura

(3) $$a' \equiv b' \pm r \pmod{p},$$

et, en multipliant (2) et (3),

(4) $$aa' \equiv bb' \pm br \pmod{p}.$$

Des congruences (1) et (4) on déduit

$$br \equiv 0 \pmod{p};$$

or p est premier avec b par hypothèse, on aura donc

$$r \equiv 0 \pmod{p},$$

ou

$$r = 0,$$

puisque $r < p$. On a donc

$$a' \equiv b' \pmod{p}.$$

Ce qu'il fallait démontrer.

Théorème de Fermat.

Si p est un nombre premier qui ne divise pas a, la différence $a^{p-1} - 1$ est divisible par p; en d'autres termes, on a

$$a^{p-1} \equiv 1 \pmod{p}.$$

Soient a et p deux nombres premiers entre eux, et considérons les $p-1$ multiples de a

$$(1) \qquad a,\ 2a,\ 3a, \ldots,\ (p-1)a;$$

l'un de ces nombres ma, par exemple, ne saurait être divisible par p, puisque p est premier avec a, et qu'il surpasse m. Il en est de même de la différence $ma - m'a$ de deux termes de la suite précédente; car cette différence est elle-même un terme de la suite. Si donc on prend les résidus minima positifs des nombres (1) par rapport à p, ces résidus seront tous différents, et aucun d'eux ne sera nul; ce seront donc, dans un certain ordre, les nombres

$$(2) \qquad 1,\ 2,\ 3, \ldots,\ (p-1).$$

Les nombres (1) étant respectivement congrus aux nombres (2), on aura, en multipliant toutes ces congruences,

$$1.2.3 \ldots (p-1)\, a^{p-1} \equiv 1.2.3 \ldots (p-1) \pmod{p}.$$

Supposons maintenant que p soit un nombre premier, on pourra diviser la dernière congruence par $1.2.3\ldots p-1$, car ce nombre est premier avec le module, et l'on aura

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ce qu'il fallait démontrer.

Théorème de Wilson.

Si p est un nombre premier, la somme $1.2.3\ldots(p-1)+1$ est divisible par p; en d'autres termes, on a

$$1.2.3\ldots(p-1) \equiv -1 \pmod{p}.$$

Soit a l'un quelconque des nombres

(1) $$1,\ 2,\ 3,\ldots,\ (p-1),$$

et formons les multiples de a

(2) $$a,\ 2a,\ 3a,\ldots,\ (p-1)a.$$

Dans la suite (2), il y a un terme congru à 1, et il n'y en a qu'un seul; supposons que ce soit αa, on aura

$$\alpha a \equiv 1 \pmod{p}.$$

Les nombres a et α sont inégaux, à moins que a ne soit égal à 1 ou à $p-1$. Si, en effet, on a $\alpha = a$, $a^2-1 = (a-1)(a+1)$ est divisible par p; or p est premier, il divise donc $a-1$ ou $a+1$, et, comme a est $< p$, on a nécessairement $a = 1$ ou $a = p-1$.

Il résulte de là que les nombres

$$2,\ 3,\ 4,\ldots,\ (p-2)$$

peuvent être associés deux à deux, de manière que le produit de deux *associés* soit congru à l'unité, et, en multipliant entre elles les congruences ainsi obtenues, on aura

$$2.3.4\ldots(p-2) \equiv 1 \pmod{p};$$

multipliant enfin par $p-1$, on a

$$1.2.3.4\ldots(p-1) \equiv p-1 \pmod{p},$$

ou

$$1.2.3.4\ldots(p-1)+1 \equiv 0 \pmod{p}.$$

Ce qu'il fallait démontrer (*).

REMARQUE. — Ce théorème est surtout remarquable en ce qu'il exprime une propriété qui appartient exclusivement aux nombres premiers; car, si p est un nombre composé, et que θ soit un de ses diviseurs, θ divisera le produit $1.2.3\ldots(p-1)$, et, par conséquent, ne pourra diviser ce même produit augmenté de l'unité. Il en sera donc de même du nombre p.

Des congruences en général.

La théorie des nombres résout sur les congruences le même problème que l'algèbre ordinaire sur les équations; elle se propose, en particulier, de trouver les valeurs de x, qui satisfont à une congruence telle que

$$f(x) \equiv 0 \pmod{p},$$

où $f(x)$ désigne un polynôme entier et rationnel dont les coefficients sont des nombres entiers. Si l'on satisfait à cette congruence, en faisant $x=a$, on y satisfera aussi, d'après une remarque précédente, en faisant, quel que soit l'entier m, $x=a+mp$; d'où il suit que chaque solution en donne une infinité d'autres, mais qui sont toutes équivalentes suivant le module p. Les diverses solutions renfermées dans une même formule $a+mp$ peuvent se

(*) Le théorème de Wilson, ainsi que celui de Fermat, est susceptible d'être généralisé; mais comme cette extension ne nous est d'aucune utilité pour l'objet auquel se rapportent les développements que nous présentons ici, nous nous bornerons à renvoyer le lecteur à l'excellent Mémoire que M. Poinsot a publié dans le tome X du *Journal de Mathématiques pures et appliquées*.

déduire de l'une quelconque d'entre elles ; d'ailleurs, on peut disposer de l'entier m de manière que $a+mp$ soit compris entre $-\frac{p}{2}$ et $+\frac{p}{2}$, ou entre o et p ; il n'y a donc lieu de s'occuper que des solutions comprises entre ces limites.

Cela posé, nous appellerons *racines* de la congruence

$$f(x) \equiv 0 \pmod{p},$$

les diverses valeurs de x comprises entre o et p, qui rendent $f(x)$ divisible par p.

Une congruence est *identique* si tous ses coefficients sont divisibles par le module, et elle est évidemment impossible si ses coefficients sont divisibles par le module, à l'exception du terme indépendant de x.

Si $\mathrm{F}(x)$ désigne un polynôme entier et rationnel, ayant pour coefficients des nombres entiers, on peut substituer à la congruence

$$f(x) \equiv 0 \pmod{p}$$

la congruence équivalente

$$f(x) + p\,\mathrm{F}(x) \equiv 0 \pmod{p},$$

et disposer ensuite des coefficients indéterminés de $\mathrm{F}(x)$, pour rabaisser au-dessous de p, et même de $\frac{p}{2}$ si l'on veut, tous les coefficients de la congruence.

Nous nous bornerons, dans ce qui va suivre, aux congruences dont le module est premier. On peut alors faire en sorte que le coefficient du premier terme soit égal à l'unité.

Considérons, en effet, la congruence

$$\mathrm{A}_0 x^m + \mathrm{A}_1 x^{m-1} + \mathrm{A}_2 x^{m-2} + \ldots \equiv 0 \pmod{p},$$

dont le module p est supposé premier, et les coefficients

A_0, A_1, A_2, etc., compris entre o et p, ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$. En ajoutant à son premier membre le polynôme

$$p(y_1 x^{m-1} + y_2 x^{m-2} + \ldots),$$

on peut l'écrire ainsi :

$$A_0 x^m + (A_1 + p y_1) x^{m-1} + (A_2 + p y_2) x^{m-2} + \ldots \equiv 0 \pmod{p},$$

ou

$$A_0 \left(x^m + \frac{A_1 + p y_1}{A_0} x^{m-1} + \frac{A_2 + p y_2}{A_0} x^{m-2} + \ldots \right) \equiv 0 \pmod{p}.$$

Cela posé, A_0 étant inférieur à p sera premier avec lui, et l'on pourra disposer des indéterminées y_1, y_2, etc., de manière que

$$\frac{A_1 + p y_1}{A_0}, \quad \frac{A_2 + p y_2}{A_0}, \ldots$$

soient des nombres entiers B_1, B_2, etc., compris entre o et p ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$; notre congruence sera donc

$$A_0 (x^m + B_1 x^{m-1} + B_2 x^{m-2} + \ldots) \equiv 0 \pmod{p},$$

ou, comme A_0 est premier avec le module,

$$x^m + B_1 x^{m-1} + B_2 x^{m-2} + \ldots \equiv 0 \pmod{p}$$

Limite du nombre des racines d'une congruence suivant un module premier.

THÉORÈME. — *Une congruence non identique, suivant un module premier, a au plus autant de racines qu'il y a d'unités dans son degré.*

Soit la congruence de degré m

(1) $$f(x) \equiv 0 \pmod{p},$$

où le coefficient du premier terme est l'unité. Supposons que a soit une racine, divisons $f(x)$ par $x-a$, et désignons par $f_1(x)$ le quotient qui est du degré $m-1$, on aura

$$f(x)=(x-a)\,f_1(x)+f(a);$$

et comme $f(a)$ est, par hypothèse, divisible par p, la congruence (1) peut s'écrire ainsi :

$$(x-a)\,f_1(x)\equiv 0 \pmod{p}.$$

Soit maintenant b une seconde racine, on aura

$$(b-a)\,f_1(b)\equiv 0 \pmod{p},$$

ou

$$f_1(b)\equiv 0 \pmod{p};$$

car $b-a$ est inférieur à p, et, par conséquent, premier avec lui ; b est donc racine de

(2) $$f_1(x)\equiv 0 \pmod{p},$$

dont le premier terme a, comme celui de (1), pour coefficient l'unité.

Il résulte de là que la congruence (1) de degré m ne peut avoir qu'une racine de plus que la congruence (2) du degré $m-1$. A son tour, cette dernière ne pourra avoir qu'une racine de plus qu'une congruence

(3) $$f_2(x)\equiv 0 \pmod{p}$$

de degré $m-2$, et dont le premier terme a pour coefficient l'unité. Par suite, la proposée (1) ne peut avoir que deux racines de plus que (3), et en continuant ce raisonnement, on fera voir que la congruence (1) ne peut avoir que $m-1$ racines de plus qu'une congruence du premier degré, telle que

$$x-l\equiv 0 \pmod{p},$$

laquelle n'admet que la seule racine l. D'où il suit, enfin,

qu'une congruence de degré m ne peut avoir plus de m racines; mais elle peut en avoir moins de m, et même n'en avoir aucune.

Corollaire I. — Supposons que la congruence de degré m

$$f(x) \equiv 0 \pmod{p},$$

dont le premier terme a pour coefficient l'unité, ait effectivement m racines

$$a,\, b,\, c, \ldots,\, k,\, l:$$

ces m racines appartiendront aussi à la congruence

$$f(x) - (x-a)(x-b)\ldots(x-l) \equiv 0 \pmod{p};$$

mais cette dernière n'est que du degré $m-1$, elle est donc identique, et, par conséquent, on a

$$f(x) = (x-a)(x-b)\ldots(x-l) + p\,F(x),$$

$F(x)$ désignant une fonction entière et rationnelle de x dont les coefficients sont des nombres entiers.

Corollaire II. — D'après le théorème de Fermat, la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

admet les $p-1$ racines

$$1,\, 2,\, 3, \ldots, (p-1).$$

Il suit de là que si $f(x)$ désigne un diviseur du binôme $x^{p-1}-1$, ou, plus généralement, un diviseur de ce même binôme augmenté d'un polynôme de degré $p-1$ tel que $p\,F(x)$, la congruence

$$f(x) \equiv 0 \pmod{p}$$

aura autant de racines qu'il y a d'unités dans son degré.

Soit, en effet,

$$x^{p-1} - 1 + p\,F(x) \equiv f(x) f_1(x);$$

la congruence de degré $p-1$

$$f(x)f_1(x) \equiv 0 \pmod{p}$$

admet les racines

$$1, 2, 3, \ldots, (p-1).$$

D'ailleurs ces racines sont celles des deux suivantes :

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p},$$

et si l'une d'elles avait moins de racines qu'il n'y a d'unités dans son degré, il faudrait que l'autre en eût plus qu'il n'y a d'unités dans le sien; ce qui est impossible.

Détermination du nombre des racines d'une congruence.

On peut déduire de ce qui précède un procédé très-simple pour déterminer le nombre des racines d'une congruence de module premier. Démontrons d'abord le lemme suivant :

LEMME. — *Si $f_2(x)$ désigne le reste de la division des deux polynômes $f(x)$ et $f_1(x)$ dont les premiers termes ont pour coefficients l'unité, les racines communes aux deux congruences*

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p}$$

sont les mêmes que les racines communes à

$$f_1(x) \equiv 0 \pmod{p}, \quad f_2(x) \equiv 0 \pmod{p}.$$

Soit Q le quotient de la division de $f(x)$ par $f_1(x)$, on aura

$$f(x) = f_1(x).Q + f_2(x),$$

et cette égalité fait voir que si $f_1(x)$ est divisible par p en même temps que l'un des deux polynômes $f(x)$ et $f_2(x)$, l'autre le sera nécessairement aussi; d'où résulte la proposition énoncée.

Corollaire. — Les racines communes à deux congruences

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p}$$

appartiennent à la congruence

$$\varphi(x) \equiv 0 \pmod{p},$$

$\varphi(x)$ désignant le plus grand commun diviseur aux deux polynômes $f(x)$ et $f_1(x)$.

Remarque. — Pour trouver ce plus grand commun diviseur $\varphi(x)$, on suivra la marche ordinaire; seulement on négligera tous les termes qui sont multipliés par p. Il faut, en outre, que toutes les divisions puissent se faire sans écrire de coefficients fractionnaires. Pour cela, on peut faire en sorte, comme il a été indiqué plus haut, que les premiers termes des restes aient tous pour coefficient l'unité. On arrive aussi au même but en multipliant chaque dividende par un facteur convenable, ou même simplement en ajoutant au coefficient du premier terme de chaque dividende un multiple de p tel, qu'après cette addition le premier terme du dividende en question soit divisible par le premier terme du diviseur correspondant.

Problème. — *Trouver le nombre des racines d'une congruence*

$$(1) \qquad f(x) \equiv 0 \pmod{p}.$$

Les racines de cette congruence appartiennent toutes à la congruence

$$(2) \qquad x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Il suffit donc de chercher les racines communes aux congruences (1) et (2). Pour cela, on prendra, comme il vient d'être dit, le plus grand commun diviseur à $f(x)$ et à $x^{p-1} - 1$. S'il n'existe pas de diviseur commun, la proposée n'aura aucune racine; si, au contraire, on trouve un plus grand commun diviseur $\varphi(x)$ de degré μ, la con-

gruence proposée aura μ racines, qui seront celles de

$$\varphi(x) \equiv 0 \quad (\text{mod. } p).$$

Cette dernière a effectivement μ racines, puisque $\varphi(x)$ est un diviseur de degré μ du binôme $x^{p-1} - 1$.

Exemple. — Supposons qu'on demande le nombre des racines de la congruence

$$x^5 - 3x^4 - 2x^3 - 2x^2 + x - 2 \equiv 0 \quad (\text{mod. } 7).$$

En divisant $x^6 - 1$ par le premier membre de la congruence proposée et négligeant les multiples de 7, on trouve pour reste

$$-3x^4 + x^3 - 2x^2 - x - 2;$$

en divisant ensuite le premier membre de la congruence proposée par ce premier reste, on trouve le deuxième reste

$$2x^3 - x^2 - 2x + 1.$$

Dans cette seconde opération, on a ajouté successivement au dividende les termes $-7x^5$ et $-7x^4$, afin d'éviter les coefficients fractionnaires.

Enfin, en divisant le premier reste par le deuxième et négligeant toujours les multiples de 7, on trouve zéro pour troisième reste. Ici il a suffi d'ajouter le terme $-7x^4$ au dividende avant de faire la division.

Il résulte de là que la congruence proposée a trois racines qui appartiennent aussi à la congruence du troisième degré

$$2x^3 - x^2 - 2x + 1 \equiv 0 \quad (\text{mod. } 7).$$

En ajoutant $7x^2 - 7$ au premier membre et divisant par 2, il vient

$$x^3 + 3x^2 - x - 3 \equiv 0 \quad (\text{mod. } 7),$$

ou

$$(x-1)(x-4)(x-6) \equiv 0 \pmod{7}.$$

La proposée admet donc les trois racines 1, 4, 6.

Nouvelle démonstration du théorème de Wilson.

Si p est premier, la congruence

$$(x-1)(x-2)(x-3)\ldots(x-p+1)-(x^{p-1}-1)\equiv 0 \pmod{p}$$

admet les $p-1$ racines

$$1, 2, 3, \ldots, (p-1);$$

et comme elle n'est que du degré $p-2$, en ordonnant son premier membre par rapport à x, les coefficients devront être tous divisibles par p. Si donc on désigne par S_1 la somme des nombres 1, 2,..., $(p-1)$, par S_2 la somme de leurs produits deux à deux, etc., par S_{p-1} le produit de tous ces nombres, on aura

$$S_1 \equiv 0, \quad S_2 \equiv 0, \quad S_3 \equiv 0, \ldots, S_{p-1} \equiv -1,$$

suivant le module p. La dernière de ces congruences constitue le théorème de Wilson.

REMARQUE. — Les coefficients de l'équation

$$(x-1)(x-2)(x-3)\ldots(x-p+1) = 0,$$

ordonnée par rapport à x, étant des multiples de p, à l'exception du dernier terme, si p est premier, la somme des puissances $m^{ièmes}$ des $p-1$ racines

$$1, 2, 3, 4, \ldots, (p-1),$$

sera divisible par p, à moins que m ne soit un multiple de $p-1$. Cela résulte immédiatement des formules de Newton.

VINGT-QUATRIÈME LEÇON.

Propriétés des racines des congruences binômes de module premier. — De l'existence des racines primitives. — Du nombre des racines primitives. — Recherche des racines primitives d'un nombre premier. — Table des racines primitives des nombres premiers inférieurs à 100. — Propriété des racines de l'équation $x^m - 1 = 0$, dont le degré m est un nombre premier.

Propriétés des racines des congruences binômes de module premier.

I. *Les racines communes à deux congruences binômes de module premier p,*

$$x^m \equiv 1 \pmod{p}, \quad x^n \equiv 1 \pmod{p},$$

sont également racines de la congruence

$$x^\theta \equiv 1 \pmod{p},$$

θ étant le plus grand commun diviseur de m et de n.

$x^\theta - 1$ est, en effet, le plus grand commun diviseur de $x^m - 1$ et de $x^n - 1$. Ce théorème est, par suite, une conséquence du corollaire démontré page 322.

Il est évident que, réciproquement, chaque racine de la congruence $x^\theta - 1 \equiv 1$ satisfait aux deux proposées.

Corollaire. — Les racines d'une congruence binôme de module premier

$$x^m \equiv 1 \pmod{p},$$

appartenant, d'après le théorème de Fermat, à la con-

gruence

$$x^{p-1} \equiv 1 \pmod{p},$$

sont aussi racines de la congruence

$$x^{\theta} \equiv 1 \pmod{p},$$

θ désignant le plus grand commun diviseur des nombres m et $p-1$.

Comme $x^{\theta}-1$ est un diviseur de $x^{p-1}-1$, cette dernière a précisément θ racines, ainsi que la proposée.

Si m est premier avec $p-1$, on a $\theta = 1$, et alors la congruence $x^m \equiv 1$ n'a d'autre racine que l'unité.

D'après ce qui précède, on peut borner l'étude des congruences binômes de la forme

$$x^m \equiv 1 \pmod{p},$$

à celles dont le degré m est un diviseur de $p-1$.

II. *Si a désigne une racine quelconque de la congruence de module premier*

$$x^m \equiv 1 \pmod{p}$$

dont le degré m est un diviseur de $p-1$, *toute puissance de a ou son résidu minimum est également racine.*

La congruence

$$a^m \equiv 1 \pmod{p}$$

entraîne, en effet,

$$a^{mk} \equiv 1 \quad \text{ou} \quad (a^k)^m \equiv 1,$$

et si b désigne le résidu minimum de a^k, par rapport à p, on a

$$a^k \equiv b, \quad \text{d'où} \quad b^m \equiv 1;$$

et, par conséquent, tous les termes de la série

$$a, \quad a^2, \quad a^3, \ldots,$$

ou leurs résidus minima, sont racines de la même congruence. Or, à cause de $a^m \equiv 1$, on a aussi

$$a^{m+1} \equiv a, \quad a^{m+2} \equiv a^2, \ldots.$$

La série précédente contient donc au plus m termes ayant des résidus différents, et ces résidus se reproduisent périodiquement de m en m. Si les m premiers termes

$$a, \; a^2, \; a^3, \ldots, \; a^{m-1}, \; a^m \quad \text{ou} \quad 1$$

sont différents (non congrus suivant le module p), leurs résidus sont les m racines de la congruence proposée. Dans le cas contraire, si l'on a, par exemple,

$$a^{n+n'} \equiv a^{n'} \pmod{p},$$

a étant premier avec p, il vient, en divisant par $a^{n'}$,

$$a^n \equiv 1 \pmod{p},$$

et, par conséquent, a est racine d'une congruence binôme

$$x^n \equiv 1 \pmod{p}$$

de degré n inférieur à m.

Il résulte de là que :

Si a est une racine de la congruence $x^m \equiv 1 \pmod{p}$, *qui n'appartienne à aucune congruence de degré moindre* $x^n \equiv 1 \pmod{p}$, *les m racines de la proposée seront les résidus des m puissances de a*

$$a, \; a^2, \; a^3, \ldots, \; a^{m-1}, \; a^m.$$

Cela posé, nous appellerons *racines primitives* d'une congruence binôme

$$x^m \equiv 1 \pmod{p}$$

dont le degré m divise $p-1$, celles des racines de cette congruence qui n'appartiennent à aucune congruence de même forme et de degré moindre. Chaque racine primitive jouit de la propriété de donner toutes les autres racines par ses diverses puissances.

REMARQUE. — Toute racine non primitive de la congruence $x^m \equiv 1 \pmod{p}$, appartenant à une congruence de même forme et de degré moindre, appartient aussi à une troisième congruence de même forme, et dont le degré divise celui de la proposée.

De l'existence des racines primitives.

Considérons la congruence

(1) $$x^m \equiv 1 \pmod{p},$$

et supposons d'abord que m ne contienne qu'un seul facteur premier q, que l'on ait

$$m = q^\mu;$$

toute racine non primitive de

(2) $$x^{q^\mu} \equiv 1 \pmod{p}$$

appartient à une congruence

$$x^\theta \equiv 1 \pmod{p},$$

dont le degré θ est un diviseur de q^μ et même de $q^{\mu-1}$; et, par conséquent, cette racine appartient aussi à la congruence

(3) $$x^{q^{\mu-1}} \equiv 1 \pmod{p}.$$

D'ailleurs les racines de (3) sont toutes racines de (2); leur nombre est $q^{\mu-1}$, par conséquent celui des racines primitives de la proposée est

$$q^\mu - q^{\mu-1}, \quad \text{ou} \quad q^\mu\left(1 - \frac{1}{q}\right).$$

Supposons maintenant m quelconque, et soit

$$m = q^{\mu} r^{\nu} \ldots s^{\lambda},$$

$q, r, \ldots, s$ désignant des facteurs premiers inégaux.

Considérons les congruences

(4) $x^{q^{\mu}} \equiv 1$ (mod. p), $x^{r^{\nu}} \equiv 1$ (mod. p),..., $x^{s^{\lambda}} \equiv 1$ (mod. p),

et désignons par a une racine primitive de la première, par b une de la seconde, etc., par c une de la dernière; je dis que le résidu du produit

$$ab \ldots c$$

est une racine primitive de la proposée

(5) $$x^{q^{\mu} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p}.$$

Il est d'abord évident que $ab\ldots c$, ou son résidu, est racine; car ayant

$$a^{q^{\mu}} \equiv 1, \quad b^{r^{\nu}} \equiv 1, \ldots, \quad c^{s^{\lambda}} \equiv 1 \pmod{p},$$

on a aussi

$$(ab\ldots c)^{q^{\mu} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p}.$$

Maintenant, si ce produit n'est pas une racine primitive de la proposée, il sera racine d'une congruence

$$x^{\theta} \equiv 1 \pmod{p},$$

dont le degré θ sera un diviseur de m, et il y aura au moins l'un des facteurs premiers de m, qui entrera dans θ moins de fois que dans m. Admettons que le facteur q soit dans ce cas; alors θ divisera $q^{\mu-1} r^{\nu} \ldots s^{\lambda}$, et, par suite, $ab\ldots c$ sera racine de la congruence

$$x^{q^{\mu-1} r^{\nu} \ldots s^{\lambda}} \equiv 1 \pmod{p};$$

on aura donc

$$(ab\ldots c)^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \pmod{p};$$

mais on a aussi

$$(b\ldots c)^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \pmod{p},$$

et, par la division,

$$a^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \pmod{p}.$$

On voit, par là, que a est racine des deux congruences

$$x^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \quad \text{et} \quad x^{q^{\mu}} \equiv 1 \pmod{p},$$

et, par suite, de

$$x^{q^{\mu-1}} \equiv 1, \pmod{p},$$

puisque $q^{\mu-1}$ est le plus grand commun diviseur entre les degrés des précédentes; a n'est donc pas, comme on l'a supposé, une racine primitive de $x^{q^{\mu}} \equiv 1 \pmod{p}$.

Il est ainsi démontré que, si $a, b, \ldots, c$ désignent des racines primitives, respectivement de la première, de la deuxième, etc., de la dernière des congruences (4), le produit $ab\ldots c$, ou son résidu, est une racine primitive de la congruence proposée (5).

Ce qui précède démontre l'existence d'une racine primitive pour toute congruence binôme de module premier

$$x^{m} \equiv 1 \pmod{p},$$

mais on n'en peut pas immédiatement conclure le nombre de ces racines. Toutefois, par des raisonnements semblables à ceux que nous avons employés dans la treizième leçon à l'occasion de l'équation binôme, on prouverait aisément que toutes les racines, tant primitives que non primitives, de la congruence (5), sont représentées par la

formule

$$ab\ldots c,$$

où l'on doit prendre pour $a, b, \ldots, c$ toutes les racines respectivement de la première des congruences (4), de la deuxième, etc., de la dernière; et que la même formule donne toutes les racines primitives, en prenant pour $a, b, \ldots, c$ les diverses racines primitives des congruences auxquelles elles appartiennent. Comme le nombre des racines primitives a est $q^{\mu}\left(1-\frac{1}{q}\right)$, que celui des racines b est $r^{\nu}\left(1-\frac{1}{r}\right), \ldots,$ celui des racines c, $s^{\lambda}\left(1-\frac{1}{s}\right)$, on en conclurait que le nombre des racines primitives de la proposée est

$$m\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right).$$

On sait que ce même nombre (*voir* la *Théorie des nombres*, ou le Mémoire déjà cité de M. Poinsot) exprime combien il y a de nombres premiers avec m et inférieurs à m.

Je ne crois pas nécessaire de développer ces raisonnements, que le lecteur trouvera aisément après avoir étudié la treizième leçon; mais j'indiquerai la démonstration ingénieuse de M. Poinsot, pour prouver qu'en admettant l'existence d'une racine primitive de la congruence

$$x^m \equiv 1 \pmod{p},$$

il y en a précisément autant que de nombres premiers avec m et inférieurs à m.

Du nombre des racines primitives.

Soit a une racine primitive de la congruence

$$x^m \equiv 1 \pmod{p},$$

et formons la suite des m puissances

$$(1) \qquad a,\ a^2,\ a^3,\ldots,\ a^{m-1},\ a^m,$$

dont les résidus sont les m racines de la proposée. Si l'on considère un nombre quelconque e inférieur à m et premier avec lui, et qu'après avoir rangé ces racines en cercle, on les considère en allant de l'une à l'autre de e en e, comme l'intervalle e par lequel on saute est premier avec m, on sera obligé de passer par toutes les racines avant de revenir à la racine a, d'où l'on est parti : donc la suite

$$a^e,\ (a^e)^2,\ (a^e)^3,\ldots,\ (a^e)^{m-1},\ (a^e)^m,$$

donne, aux multiples près de p, toutes les racines de la proposée; donc a^e est une racine primitive.

Si le nombre e, que nous avons supposé premier avec p, avait avec lui un plus grand commun diviseur $\theta > 1$, en opérant, sur la suite (1), comme nous venons de le faire, on ne passerait jamais que par un nombre $\frac{m}{\theta}$ de racines, et, par conséquent, a^e ne serait pas une racine primitive.

Il suit évidemment de là que la congruence proposée a autant de racines primitives qu'il y a de nombres premiers avec m et inférieurs à m.

Recherche des racines primitives d'un nombre premier.

On nomme *racines primitives d'un nombre premier p* les racines primitives de la congruence binôme de degré $p-1$,

$$x^{p-1} \equiv 1 \pmod{p}.$$

THÉORÈME. — *Soient x_1 et ξ deux nombres compris entre 0 et p, et θ un diviseur de $p-1$; si l'on a*

$$x_1^\theta \equiv \xi \pmod{p},$$

on a aussi

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p};$$

et, réciproquement, si l'on a

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p},$$

la congruence

$$x^\theta \equiv \xi \pmod{p}$$

a θ racines.

La première partie du théorème est évidente; car, si l'on a

$$x_1^\theta \equiv \xi \pmod{p},$$

en élevant les deux membres à la puissance $\frac{p-1}{\theta}$, on a

$$x_1^{p-1} \equiv \xi^{\frac{p-1}{\theta}} \pmod{p},$$

et, à cause du théorème de Fermat,

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p}.$$

Réciproquement, supposons que l'on ait $\xi^{\frac{p-1}{\theta}} \equiv 1$, ou

$$\xi^{\frac{p-1}{\theta}} - 1 = pQ;$$

retranchant chaque membre de cette égalité de $x^{p-1} - 1$, il vient

$$x^{p-1} - 1 - pQ = x^{p-1} - \xi^{\frac{p-1}{\theta}} = (x^\theta)^{\frac{p-1}{\theta}} - \xi^{\frac{p-1}{\theta}}.$$

Or le second membre admet pour diviseur $x^\theta - \xi$; il en est donc de même du premier membre $x^{p-1} - 1 - pQ$, et, par conséquent, en vertu d'un théorème démontré

dans la dernière leçon (page 320), la congruence

$$x^{\theta} - \xi \equiv 0 \pmod{p}$$

a θ racines. Ce qu'il fallait démontrer.

Corollaire. — Si p est un nombre premier, et qu'en décomposant $p - 1$ en facteurs premiers, on ait

$$p - 1 = 2^{\rho} q^{\mu} r^{\nu} \ldots s^{\lambda},$$

les racines non primitives de la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

lesquelles appartiennent nécessairement à l'une des congruences

$$x^{\frac{p-1}{2}} \equiv 1, \quad x^{\frac{p-1}{q}} \equiv 1, \quad x^{\frac{p-1}{r}} \equiv 1, \ldots, \quad x^{\frac{p-1}{s}} \equiv 1,$$

sont, en vertu du théorème précédent, des résidus de carrés (*), ou de puissances q, ou de puissances r, etc., ou de puissances s; et, réciproquement, tout nombre résidu d'un carré, ou d'une puissance q, ou etc., est racine de l'une des congruences précédentes et n'est pas racine primitive du nombre premier p.

On voit aussi que, parmi les nombres

$$1, 2, 3, \ldots, p - 1,$$

il y en a la moitié qui sont des carrés (résidus de carrés), la $q^{\text{ième}}$ partie qui sont des puissances q, la $r^{\text{ième}}$ partie des puissances r, etc., la $s^{\text{ième}}$ partie des puissances s; et,

(*) Les résidus de carrés ou de cubes suivant un module p sont dits *résidus quadratiques* et *cubiques* de p; ils jouent un rôle important dans la théorie des nombres.

plus généralement, si l'on ne considère parmi ces nombres que ceux qui sont à la fois des puissances 2, q, r,..., la $s^{ième}$ partie de ces derniers sera en même temps des puissances s. En effet, les nombres qui sont à la fois des résidus de carrés de puissances q, de puissances r, etc., satisfont aux congruences

$$x^{\frac{p-1}{2}} \equiv 1, \quad x^{\frac{p-1}{q}} \equiv 1, \quad x^{\frac{p-1}{r}} \equiv 1, \ldots, \quad (\text{mod. } p),$$

et, par conséquent, sont racines de

$$x^{\frac{p-1}{2qr\ldots}} \equiv 1 \quad (\text{mod. } p):$$

leur nombre est donc $\frac{p-1}{2qr\ldots}$; pareillement, le nombre de ceux qui sont en même temps des puissances s est $\frac{p-1}{2qr\ldots s}$, il est donc la $s^{ième}$ partie du premier.

PROBLÈME. — *Trouver les racines primitives d'un nombre premier.*

Le théorème que nous venons de démontrer fournit un moyen très-simple de trouver les racines primitives d'un nombre premier.

Soient p un nombre premier; 2, q, r,..., s les facteurs premiers inégaux de $p-1$, et écrivons les $p-1$ nombres

$$1, \; 2, \; 3, \; 4, \ldots, \; p-1;$$

si l'on enlève de cette suite tous les résidus de carrés, de puissances q, de puissances r, etc., il ne restera plus que les racines primitives de p.

Au moyen des carrés, on exclut d'abord la moitié des nombres, ainsi que nous l'avons établi plus haut; au moyen des puissances q, on exclura la $q^{ième}$ partie de ceux qui restent, et ainsi de suite. Cette méthode, pour trouver

les racines primitives d'un nombre premier, fournit une démonstration nouvelle du théorème relatif au nombre de ces racines; ce nombre sera, en effet, d'après ce qui précède,

$$(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right).$$

Nous allons montrer, par deux exemples, comment il faut faire l'application du procédé qu'on vient d'indiquer.

Premier exemple. — *Trouver les racines primitives de* 17.

Nous écrivons d'abord les seize nombres

(1) 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,

et comme 16 n'admet que le facteur premier 2, il suffit d'ôter de cette suite les nombres qui sont résidus quadratiques. Pour cela, nous élèverons ces nombres au carré; mais, comme on a généralement

$$(17-h)^2 \equiv h^2 \pmod{17},$$

les huit derniers carrés donneront les mêmes résidus que les huit premiers : il suffit donc d'élever au carré les huit premiers, on trouvera ainsi

1, 4, 9, 16, 25, 36, 49, 64,

qui ont pour résidus

1, 4, 9, 16, 8, 2, 15, 13,

et en effaçant ces huit résidus de la suite (1), il restera les huit racines primitives de 17, savoir

3, 5, 6, 7, 10, 11, 12, 14.

Second exemple. — *Trouver les racines primitives de* 31.

Écrivons les trente nombres

$$(1)\quad \begin{cases} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, \\ 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18, & 19, & 20, \\ 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28, & 29, & 30; \end{cases}$$

comme les facteurs premiers de 30 sont 2, 3 et 5, il suffira d'enlever de la suite (1) les résidus des carrés, des cubes et des cinquièmes puissances.

Pour exclure les carrés, nous élèverons les quinze premiers nombres (1) au carré, ce qui donne

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\\ 121,\ 144,\ 169,\ 196,\ 225;$$

ces carrés ont pour résidus

(2) 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8;

ôtant ces quinze nombres (2) de la suite (1), il restera les quinze que voici :

(3) 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30,

dont il faut maintenant supprimer les cubes et les cinquièmes puissances. Chaque nombre déjà supprimé (2) satisfait à la congruence

$$x^{15} \equiv 1 \pmod{31};$$

donc sa puissance troisième et sa puissance cinquième y satisfont aussi, et, par conséquent, font partie des nombres déjà supprimés. D'après cela, les nombres de la suite (3) qu'il reste à rejeter sont des résidus de puissances troisième et cinquième de ces mêmes nombres (3). Pour avoir les résidus des cubes de la suite (3), il suffit de multiplier les premières puissances par les résidus carrés que la

suite (2) fait connaître, et qui sont

9, 5, 28, 20, 14, 8, 10, 7, 19, 2, 18, 25, 16, 4, 1;

on aura ainsi les résidus cubiques suivants :

27, 30, 308, 240, 182, 120, 170, 147, 418,
46, 432, 650, 432, 116, 30,

dont les résidus minima sont

(4) $\begin{cases} 27, 30, 29, 23, 27, 27, 15, 23, \\ 15, 15, 29, 30, 29, 23, 30. \end{cases}$

Il n'y en a que cinq de différents, comme nous le savions d'avance; ce sont

(5) 15, 23, 27, 29, 30,

et en ôtant ces nombres de la suite (3), il ne restera plus que les dix suivants :

(6) 3, 6, 11, 12, 13, 17, 21, 22, 24, 26,

dont il n'y a plus à rejeter que ceux qui sont des cinquièmes puissances. Chacun des nombres déjà exclus satisfait à l'une des congruences

$$x^{15} \equiv 1 \pmod{31}, \quad x^{10} \equiv 1 \pmod{31}.$$

Il en est donc de même de sa cinquième puissance, qui, par conséquent, fait partie des nombres exclus : un nombre de la suite (6) ne peut donc être la cinquième puissance que d'un nombre de la même suite. Pour avoir les résidus des cinquièmes puissances des nombres (6), il suffit de multiplier les résidus cubiques déjà formés par les résidus quadratiques correspondants, et de prendre les résidus minima des produits. Les résidus cubiques sont

27, 30, 29, 23, 27, 15, 23, 15, 29, 30,

les quadratiques

9, 5, 28, 20, 14, 10, 7, 19, 18, 25;

les produits sont

243, 150, 812, 460, 378, 150, 161, 285, 522, 750,

et l'on trouve pour résidus des cinquièmes puissances,

26, 26, 6, 26, 6, 26, 6, 6, 26, 6.

Il n'y a ainsi, dans la suite (6), que deux cinquièmes puissances, comme nous le savions déjà, savoir

6, 26;

en supprimant ces deux nombres, il ne restera plus que les huit racines primitives de 31, savoir

3, 11, 12, 13, 17, 21, 22, 24.

La Table suivante renferme les racines primitives des nombres premiers inférieurs à 100 :

Table des racines primitives des nombres premiers inférieurs à 100.

NOMBRES premiers.	NOMBRE des racines primitives.	RACINES PRIMITIVES.
3	1	2.
5	2	2.3.
7	2	3.5.
11	4	2.6.7 8.
13	4	2.6.7.11.
17	8	3.5.6.7.10.11.12.14.
19	6	2.3.10.13.14.15.
23	10	5.7.10.11.13.14.15.17.20.21.
29	12	2.3.8.10.11.14.15.18.19.21.26.27.
31	8	3.11.12.13.17.21.22.24.
37	12	2.5.13.15.17.18.19.20.22.24 32.35.
41	16	6.7.11.12.13.15.17.19.22.24.26.28.29.30.34.35.
43	12	3.5.12.18.19.20.26.28.29.30.33.34
47	22	5.10.11.13.15.19.20.22.23.26.29.30.31.33.35.38. 39.40.41.43.44.45.
53	24	2.3.5.8.12.14.18.19.20.21.22.26.27.31.32.33.34. 35.39.41.45.48.50.51.
59	28	2.6.8.10.11.13.14.18.23.24.30.31.32.33.34.37.38. 39.40.42.43.44.47.50.52.54.55.56
61	16	2.6.7.10.17.18.26.30.31.35.43.44.51.54.55.59.
67	20	2.7.11.12.13.18.20.28.31.32.34.41.44.46.48.50. 51.57.61.63.
71	24	7.11.13.21.22.28.31.33.35.42.44.47.52.53.55.56. 59.61.62.63.65.67.68.69.
73	24	5.11.13.14.15.20.26.28.29.31.33.34.39.40.42.44. 45.47.53.58.59 60.62.68.
79	24	3.6.7.28.29.30.34.35.37.39.43.47 48 53.54.59.60. 63.66.68.70.74 75.77.
83	40	2.5.6.8.13.14.15.18.19.20.22.24.32.34.35.39.42. 43.45.46.47.50.52.53.54.55.56 57.58.60.62.66.67. 71.72.73 74.76.79.80.
89	40	3.6.7.13.14.15.19.23.24.26.27.28.29.30.31.33.35. 38.41.43.46.48.51.54.56.58 59.60.61.62.63.65.66. 70.74.75.76.82.83.86.
97	32	5.7.10.13.14.15.17.21.23.26.29.37.38.39 40.41. 56.57.58.59.66.68.71.74.76.80.82.83.84.87.90.92.

Propriétés des racines de l'équation $\frac{x^m - 1}{x - 1} = 0$, *où* m *est premier.*

Soit α une racine imaginaire de l'équation

(1) $$x^m - 1$$

de degré m premier; les $m - 1$ racines de l'équation

(2) $$\frac{x^m - 1}{x - 1} = 0$$

sont, comme on sait,

$$\alpha,\quad \alpha^2,\quad \alpha^3,\ldots,\quad \alpha^{m-1}.$$

Soit maintenant a une racine primitive du nombre premier m ou de la congruence

$$x^{m-1} \equiv 1 \pmod{m};$$

les $m - 1$ racines de cette congruence, savoir

$$1,\quad 2,\quad 3,\ldots,\quad (m-1),$$

peuvent être représentées par les diverses puissances de a,

$$1,\quad a,\quad a^2,\ldots,\quad a^{m-2},$$

aux multiples près de m; et, par conséquent, les $m - 1$ racines de l'équation (2) sont

$$\alpha,\quad \alpha^a,\quad \alpha^{a^2},\ldots,\quad \alpha^{a^{m-2}},$$

en sorte que chacune d'elles s'obtient en élevant la précédente à la puissance a; et la même chose a lieu encore à cause de $a^{m-1} \equiv 1$ (mod. m), si l'on range en cercle ces m racines, et que l'on considère successivement chacune d'elles comme étant la première. D'après cela, si x

désigne l'une quelconque des racines de l'équation (2), et que l'on fasse

$$x^a = \theta(x), \quad \theta\theta(x) = \theta^2(x), \quad \theta\theta^2(x) = \theta^3(x), \ldots$$

les *m* racines de l'équation (2) seront représentées par

$$x, \quad \theta(x), \quad \theta^2(x), \ldots, \quad \theta^{m-2}(x),$$

et l'on aura

$$\theta^{m-1}(x) = x.$$

C'est sur cette propriété que repose la méthode de M. Gauss pour la résolution de l'équation (2), dont nous nous occuperons dans une prochaine leçon.

VINGT-CINQUIÈME LEÇON.

Des congruences irréductibles suivant un module premier. — Des nouvelles quantités imaginaires qui naissent de la théorie des nombres — Des racines d'une congruence irréductible. — De la congruence $x^{p^\nu} - x \equiv 0$ (mod. p). — Propriété des racines d'une congruence irréductible. — Des racines primitives. — Recherche de toutes les racines d'une congruence quelconque. — Application de la théorie à un exemple

Des congruences irréductibles suivant un module premier.

Soient p un nombre premier et $F(x)$ une fonction entière de x à coefficients entiers. La congruence

$$F(x) \equiv 0 \quad (\text{mod. } p)$$

est dite *irréductible*, s'il est impossible de trouver trois polynômes $\varphi(x)$, $\psi(x)$, $\chi(x)$ à coefficients entiers et qui soient tels, que l'on ait identiquement

$$\varphi(x)\psi(x) = F(x) + p\chi(x).$$

Quelle que soit la congruence

$$F(x) \equiv 0 \quad (\text{mod. } p),$$

on peut toujours supposer les coefficients inférieurs au module, et, si le module est premier, ce qui est le seul cas dont nous ayons à nous occuper, on peut faire en sorte que le coefficient du terme le plus élevé en x soit l'unité, ainsi que cela a été expliqué dans la vingt-troisième le-

çou. Nous supposerons toujours que les congruences que nous aurons à considérer, dans ce qui va suivre, soient préparées de cette manière.

Si la congruence

$$F(x) \equiv 0 \pmod{p}$$

n'est pas irréductible, on pourra décomposer son premier membre en facteurs *irréductibles*; en d'autres termes, on aura

$$\varphi(x)\psi(x)\ldots\varpi(x) = F(x) + p\chi(x),$$

$\varphi(x)$, $\psi(x)$,..., $\varpi(x)$ étant des polynômes égaux ou inégaux et à coefficients entiers moindres que p, tels, en outre, que les congruences

$$\varphi(x) \equiv 0, \quad \psi(x) \equiv 0, \ldots, \quad \varpi(x) \equiv 0 \pmod{p}$$

soient irréductibles. Il faut remarquer que, si quelques-uns des polynômes $\varphi(x)$, $\psi(x)$, etc., sont égaux entre eux, la congruence proposée aura nécessairement un diviseur commun avec sa dérivée. Car soit

$$\varphi(x)^m \Phi(x) = F(x) + p\chi(x),$$

on aura, en prenant les dérivées des deux membres,

$$\varphi(x)^{m-1}[m\varphi'(x)\Phi(x) + \varphi(x)\Phi'(x)] = F'(x) + p\chi'(x).$$

Si donc on cherche le plus grand commun diviseur des polynômes $F(x)$ et $F'(x)$, en négligeant toujours les termes multipliés par p, on trouvera un diviseur commun fonction de x.

Théorème. — *Si*

$$F(x) \equiv 0 \pmod{p}$$

est une congruence irréductible, suivant un module pre-

mier, et si l'on a identiquement

(1) $$\varphi(x)\psi(x) = F(x)f(x) + p\chi(x),$$

φ, ψ, f désignant des fonctions entières de x dont les coefficients sont des entiers inférieurs à p, et χ une fonction entière à coefficients entiers, mais quelconques; on aura aussi

(2) $$\varphi(x) = F(x)f_1(x) + p\chi_1(x),$$

ou

(3) $$\psi(x) = F(x)f_1(x) + p\chi_1(x),$$

f_1 et χ_1 étant des fonctions entières de x.

Supposons que l'on n'ait pas

$$\varphi(x) = F(x)f_1(x) + p\chi_1(x),$$

je dis que l'on aura

$$\psi(x) = F(x)f_1(x) + p\chi_1(x).$$

Pour le démontrer, soit r le coefficient de la plus haute puissance de x dans $\varphi(x)$; en ajoutant à $\varphi(x)$ un polynôme de la forme $p\lambda(x)$ de degré inférieur au sien, on pourra rendre tous les termes divisibles par r, en sorte que l'on aura

(4) $$\varphi(x) \equiv rR \pmod{p}.$$

Cela posé, les premiers termes des polynômes $F(x)$ et R ayant pour coefficient l'unité, faisons sur ces polynômes l'opération du plus grand commun diviseur, en ayant soin d'ajouter à chaque reste un polynôme de la forme $p\lambda(x)$ choisi de manière qu'après cette addition, le reste en question soit divisible par le coefficient du terme le plus élevé; en outre, avant de prendre ce reste pour diviseur, nous supprimerons le facteur com-

mun à tous ses termes. Comme on admet que l'égalité (2) ne peut avoir lieu, on arrivera nécessairement à un reste numérique r_n qui ne sera pas nul suivant le module p. Et si l'on suppose, pour fixer les idées, que le degré de $F(x)$ ne soit pas inférieur à celui de $\varphi(x)$ ou R, on aura cette suite d'égalités ou de congruences,

$$(5)\qquad \left\{\begin{array}{l} F(x) \equiv RQ_1 + r_1 R_1, \\ R \equiv R_1 Q_2 + r_2 R_2, \\ \dots\dots\dots\dots \\ R_{n-2} \equiv R_{n-1} Q_n + r_n. \end{array}\right. \pmod{p},$$

$r_1, r_2, \ldots, r_n$ sont des entiers qui ne sont pas nuls suivant le module p; et $R_1, R_2, \ldots, Q_1, Q_2, \ldots$, sont des fonctions entières de x dans lesquelles le terme le plus élevé en x a pour coefficient l'unité. Des relations (4) et (5), on déduit

$$\left\{\begin{array}{l} rr_1 R_1 \equiv rF(x) - Q_1 \varphi(x), \\ rr_1 r_2 R_2 \equiv (r_1 + Q_1 Q_2)\varphi(x) - rQ_2 F(x) \quad \pmod{p}; \\ \dots\dots\dots\dots\dots\dots \end{array}\right.$$

la dernière de ces relations aura la forme

$$rr_1 r_2 \ldots r_n \equiv MF(x) - N\varphi(x) \pmod{p},$$

ou

$$(6)\qquad \alpha + pP = MF(x) - N\varphi(x),$$

M, N, P désignant des fonctions entières de x, et α un nombre entier différent de zéro et inférieur à p. Il est évident qu'on serait arrivé au même résultat si l'on eût supposé le degré de $F(x)$ inférieur à celui de $\varphi(x)$.

Des égalités (1) et (6), on déduit

$$[\varphi(x)\psi(x) - F(x) f(x)](\alpha + pP) = p\chi(x)[MF(x) - N\varphi(x)],$$

ou

$$\varphi(x)[\alpha\psi(x) + pP\psi(x) + pN\chi(x)]$$
$$= F(x)[(\alpha + pP)f(x) + pM\chi(x)].$$

Or, par notre hypothèse, le polynôme $F(x)$ ne saurait avoir aucun facteur commun avec $\varphi(x)$, donc il divise

$$\alpha\psi(x) + p[P\psi(x) + N\chi(x)],$$

on a donc

$$\alpha\psi(x) = F(x)f_1(x) + p\chi_1(x),$$

f_1 et χ_1 étant des fonctions entières. On peut supposer que les coefficients de $f_1(x)$ soient rabaissés au-dessous de p et qu'ils soient tous divisibles par le coefficient de la plus haute puissance de x; alors, comme le premier terme de $F(x)f_1(x)$ doit détruire le premier terme de $\alpha\psi(x)$, il faut que $f_1(x)$ soit divisible par α, par conséquent $\chi_1(x)$ le sera aussi. Supprimant donc ce facteur α, on aura une égalité de la forme

$$\psi(x) = F(x)f_1(x) + p\chi_1(x),$$

ce qui démontre le théorème énoncé.

Corollaire I. — *Si*

$$F(x) \equiv 0 \pmod{p}$$

est une congruence irréductible suivant un module premier, et si l'on a identiquement

$$\varphi_1(x)\varphi_2(x)\ldots\varphi_n(x) = F(x)f(x) + p\chi(x),$$

$\varphi_m(x)$ et $f(x)$ étant des fonctions entières de x à coefficients entiers moindres que p, $\chi(x)$ étant aussi une fonction entière, on aura, pour une valeur de m au moins,

$$\varphi_m(x) = F(x)f_1(x) + p\chi_1(x),$$

f_1 et χ_1 désignant des fonctions entières.

Cette proposition se déduit immédiatement du théorème qu'on vient d'établir.

COROLLAIRE II. — *Le premier membre d'une congruence*

$$F(x) \equiv 0 \pmod{p}$$

de module premier, ne peut être décomposé que d'une seule manière en facteurs irréductibles.

Des nouvelles quantités imaginaires qui naissent de la théorie des nombres.

Soient p un nombre premier et

$$F(x) \equiv 0 \pmod{p}$$

une congruence irréductible d'un degré ν supérieur à 1.

La congruence proposée n'a aucune racine entière; mais si l'on trouve un avantage quelconque à introduire dans le calcul une *quantité* i assujettie à la condition de vérifier la congruence

$$F(i) \equiv 0 \pmod{p},$$

on devra regarder cette quantité i comme un symbole imaginaire d'une nouvelle espèce. Et, comme on peut faire en sorte que le coefficient de i^ν dans $F(i)$ soit l'unité, on voit qu'en négligeant tous les termes qui sont multipliés par p, la puissance $\nu^{ième}$ de i pourra s'exprimer, au moyen de $F(i) \equiv 0$, par une fonction entière de i du degré $\nu - 1$. La même chose aura lieu pour toutes les puissances de i supérieures à la $(\nu - 1)^{ième}$, en sorte que toute fonction entière de i pourra se mettre sous la forme

$$a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

$a_0, a_1, \ldots, a_{\nu-1}$ étant des nombres entiers qu'on peut rabaisser au-dessous de p en négligeant tous les termes mul-

tipliés par p. Pour réduire à cette forme une fonction entière de i, le plus simple sera, en général, de diviser la fonction donnée par $F(i)$ et de pousser l'opération jusqu'à ce qu'on obtienne un reste de degré inférieur à ν; ce reste sera la valeur réduite de la fonction donnée. L'expression

$$a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1}$$

est l'expression la plus générale des nouvelles quantités imaginaires qui naissent de la théorie des nombres; leur introduction dans l'analyse est due à Galois. Nous allons développer ici, à notre point de vue, les résultats que ce grand géomètre a obtenus et qu'il a indiqués succinctement dans le *Bulletin des Sciences mathématiques* de Férussac (tome XIII, page 398) (*).

D'après le théorème établi plus haut, si

$$\varphi_1(x), \quad \varphi_2(x), \ldots, \quad \varphi_n(x)$$

sont des fonctions entières de x, et si l'on a

$$\varphi_1(i)\varphi_2(i)\ldots\varphi_n(i) \equiv 0 \pmod{p},$$

c'est-à-dire

$$\varphi_1(i)\varphi_2(i)\ldots\varphi_n(i) = F(i)f(i) + p\chi(i),$$

f et χ étant des fonctions entières; une au moins des quantités $\varphi_1(i)$, $\varphi_2(i)$, etc., sera congrue à zéro suivant le module p. Nous ferons dans la suite un fréquent usage de cette proposition.

Les quantités imaginaires que nous considérons comprennent, comme cas particulier, les nombres entiers.

(*) L'article publié par Galois en 1830 dans le Bulletin de Férussac a été réimprimé ensuite avec ses autres Mémoires dans le tome XI du *Journal de Mathématiques pures et appliquées*.

Aussi le théorème fondamental que nous avons démontré dans la vingt-troisième leçon et qui est relatif au nombre des racines entières d'une congruence, est-il un cas particulier du théorème suivant que nous allons établir.

Théorème. — *Si p est un nombre premier et que i désigne une racine de la congruence irréductible de degré* ν,

$$(1)\qquad F(x) \equiv 0 \pmod{p},$$

une congruence de degré m non identique, telle que

$$(2)\qquad \varphi(x) \equiv 0 \pmod{p},$$

ne peut avoir plus de m racines distinctes ayant la forme

$$(3)\qquad a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

où a_0, a_1, *etc., désignent des entiers inférieurs à p.*

On peut employer, pour démontrer ce théorème général, le raisonnement qui nous a servi dans la vingt-troisième leçon, pour établir le théorème analogue relatif aux racines entières.

Supposons que la congruence (2) admette une racine α de la forme (3), on aura

$$\varphi(\alpha) \equiv 0 \pmod{p};$$

si donc $\varphi_1(x)$ désigne le quotient de la division de $\varphi(x)$ par $x - \alpha$, la congruence (2) pourra s'écrire comme il suit :

$$(x - \alpha)\varphi_1(x) \equiv 0 \pmod{p}.$$

Si la congruence (2) admet une deuxième racine β différente de α, mais de même forme, on aura

$$(\beta - \alpha)\varphi_1(\beta) \equiv 0 \pmod{p};$$

mais $\beta - \alpha$ étant différent de zéro et d'un degré inférieur

à ν, on ne peut avoir

$$6 - \alpha \equiv 0 \pmod{p},$$

donc on a

$$\varphi_1(6) \equiv 0 \pmod{p}.$$

Il suit de là que 6 est racine de la congruence

$$(4) \qquad \varphi_1(x) \equiv 0 \pmod{p}.$$

Le raisonnement qui précède ne suppose pas que les coefficients de la congruence (2) soient entiers, mais seulement qu'ils soient de la forme (3). Ce raisonnement prouve que la congruence (2) de degré m ne peut avoir qu'une racine de plus que la congruence (4) de degré $m-1$. A son tour, cette dernière ne peut avoir qu'une racine de plus qu'une congruence

$$(5) \qquad \varphi_2(x) \equiv 0 \pmod{p}$$

de degré $m-2$; par suite, la congruence (2) ne peut avoir que deux racines de plus que (5), et, en poursuivant ce raisonnement, on fera voir que la congruence (2) ne peut avoir que $m-1$ racines de plus qu'une congruence du premier degré, laquelle n'admet évidemment qu'une seule racine. D'où il suit enfin que la congruence (2) ne peut admettre plus de m racines de la forme (3).

Corollaire. — Supposons que la congruence (2), savoir

$$\varphi(x) \equiv 0 \pmod{p}$$

ait effectivement m racines distinctes $\alpha, 6, \ldots, \omega$ de la forme (3), la congruence

$$\varphi(x) - (x-\alpha)(x-6)\ldots(x-\omega) \equiv 0 \pmod{p}$$

admettra ces mêmes racines; or celle-ci n'est que du degré $m-1$, donc elle doit être identique, et l'on a

$$\varphi(x) = (x-\alpha)(x-6)\ldots(x-\omega) + p\chi(x),$$

$\chi(x)$ étant un polynôme dont les coefficients sont des fonctions entières de i.

Des racines d'une congruence irréductible.

Soient p un nombre premier et

$$(1) \qquad F(x) \equiv 0 \pmod{p}$$

une congruence irréductible du degré ν. Soit i une racine de cette congruence, et posons

$$A = a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

a_0, a_1, etc., étant des entiers compris entre les limites 0 et $p-1$, ou, si l'on veut, entre les limites $-\frac{p-1}{2}$ et $+\frac{p-1}{2}$. Chacun de ces coefficients a étant ainsi susceptible de p valeurs distinctes, l'expression de A pourra prendre p^ν valeurs distinctes; l'une de ces valeurs sera zéro, nous en ferons abstraction et nous considérerons seulement les $p^\nu - 1$ valeurs de A différentes de zéro.

Si α, β, γ, etc., désignent des valeurs de A égales ou inégales entre elles, le produit $\alpha\beta\gamma\ldots$ sera une fonction entière de i dont on pourra rabaisser le degré au-dessous de ν à l'aide de $F(i) \equiv 0$, et ramener les coefficients entre les limites 0 et $p-1$ ou $-\frac{p-1}{2}$ et $\frac{p-1}{2}$; ce produit sera donc aussi une valeur de A, et il ne sera jamais nul, car pour que l'on eût

$$\alpha\beta\gamma\ldots \equiv 0 \pmod{p},$$

il faudrait que l'une des quantités α, β, γ, etc., fût congrue à zéro suivant le module p, ce qui est contre l'hypothèse.

Cela posé, soit α l'une des valeurs de A; toutes les puissances de α, savoir :

$$\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ldots,$$

seront aussi des valeurs de A. Mais, parce que A n'a que $p^\nu - 1$ valeurs distinctes, il faut que quelques-unes de ces valeurs se trouvent reproduites une infinité de fois dans la série des puissances de α. Supposons que l'on ait

$$\alpha^{n+n'} \equiv \alpha^{n'} \pmod{p}, \quad \text{ou} \quad \alpha^{n'}(\alpha^n - 1) \equiv 0 \pmod{p}.$$

Comme $\alpha^{n'}$ ne peut être zéro suivant le module p, il faut que l'on ait

$$\alpha^n \equiv 1 \pmod{p},$$

et, par suite,

$$\alpha^{2n} \equiv 1,\quad \alpha^{3n} \equiv 1,\ldots,\quad \pmod{p}.$$

Il y a donc une infinité de puissances de α qui se réduisent à l'unité. Soit n le plus petit nombre qui soit tel, que l'on ait

$$\alpha^n \equiv 1 \pmod{p},$$

on aura ces n valeurs distinctes de A, savoir :

(2) $$1,\ \alpha,\ \alpha^2,\ \alpha^{n-1}.$$

Si l'on a $p^\nu - 1 = n$, les quantités (2) seront toutes les valeurs de A. Si l'on a $p^\nu - 1 > n$, soit β l'une des valeurs de A qui ne font pas partie des quantités (2); en multipliant ces quantités (2) par β, on obtient les n nouvelles valeurs suivantes de A :

(3) $$\beta,\ \alpha\beta,\ \alpha^2\beta,\ldots,\ \alpha^{n-1}\beta.$$

Ces valeurs sont différentes entre elles, car soient n' et n'' deux nombres inférieurs à n; si l'on avait

$$\alpha^{n'}\beta - \alpha^{n''}\beta \equiv 0 \pmod{p},$$

comme on ne peut avoir $6 \equiv 0 \pmod{p}$, on aurait

$$\alpha^{n'} - \alpha^{n''} \equiv 0 \pmod{p},$$

ce qui est contre l'hypothèse. En outre, les quantités (3) sont distinctes de (2); car si l'on avait, par exemple,

$$\alpha^{n'} 6 \equiv \alpha^{n''} \pmod{p},$$

on aurait, en multipliant par $\alpha^{n-n'}$,

$$\alpha^n 6 \equiv \alpha^{n-n'+n''} \quad \text{ou} \quad 6 \equiv \alpha^{n-n'+n''} \pmod{p},$$

ce qui est contre l'hypothèse.

Il résulte de là que $p^\nu - 1$ est égal ou supérieur à $2n$. Si $p^\nu - 1$ est plus grand que $2n$, soit γ une nouvelle valeur de A; en multipliant par γ les quantités (2), on obtient les nouvelles valeurs suivantes de A :

$$(4) \qquad \gamma, \ \alpha\gamma, \ \alpha^2\gamma, \ldots, \ \alpha^{n-1}\gamma.$$

Le raisonnement que nous venons de faire prouve que ces quantités (4) sont différentes entre elles et distinctes des quantités (2); il est aisé de voir aussi qu'elles sont distinctes des quantités (3), car si l'on avait, par exemple,

$$\alpha^{n'}\gamma \equiv \alpha^{n''} 6 \pmod{p},$$

en multipliant par $\alpha^{n-n'}$, il viendrait

$$\alpha^n\gamma \equiv \alpha^{n-n'+n''} 6 \quad \text{ou} \quad \gamma \equiv \alpha^{n-n'+n''} 6 \pmod{p},$$

ce qui est contre l'hypothèse.

Il résulte de là que $p^\nu - 1$ est égal ou supérieur à $3n$. Et, en poursuivant ce raisonnement, on voit que $p^\nu - 1$ est nécessairement un multiple de n. Par suite, la congruence

$$\alpha^n \equiv 1 \pmod{p}$$

entraîne nécessairement

$$\alpha^{p^{\nu}-1} - 1 \equiv 0 \pmod{p}.$$

Et comme, en particulier, i est l'une des valeurs que peut prendre A, on peut faire $\alpha = i$, et l'on voit que l'on a

$$i^{p^{\nu}-1} - 1 \equiv 0 \pmod{p},$$

c'est-à-dire

$$f(i)\,F(i) = i^{p^{\nu}-1} - 1 + p\chi(i),$$

f et χ désignant des fonctions entières.

Ce résultat, dégagé de la considération des imaginaires, se traduit dans le théorème d'algèbre suivant :

Théorème. — *Si p est un nombre premier et que $F(x) = x^{\nu} + P_1 x^{\nu-1} + P_2 x^{\nu-2} + \ldots$ soit un polynôme du degré ν à coefficients entiers, tel, qu'on ne puisse avoir*

$$\varphi(x)\,\psi(x) = F(x) + p\chi(x),$$

$\varphi(x)$, $\psi(x)$ et $\chi(x)$ étant des polynômes à coefficients entiers, on pourra poser

$$f(x)\,F(x) = x^{p^{\nu}-1} - 1 + p\chi(x),$$

ou, si l'on veut,

$$f(x)\,F(x) = x^{p^{\nu}} - x + p\chi(x),$$

f et χ désignant des polynômes à coefficients entiers.

L'égalité

$$f(x)\,F(x) = x^{p^{\nu}} - x + p\chi(x)$$

va nous permettre de démontrer que la congruence proposée

$$F(x) \equiv 0 \pmod{p}$$

admet ν racines distinctes de la forme A.

Remarquons d'abord que les coefficients de $f(x)$ pouvant être rabaissés au-dessous de p, le degré de $f(x)\,F(x)$ est nécessairement égal à p^ν. Cela posé, d'après ce qui précède, la congruence

$$x^{p^\nu} - x \equiv 0 \pmod{p}$$

admet pour racines les p^ν valeurs de A, zéro compris; d'ailleurs les racines de cette congruence appartiennent à l'une ou à l'autre des deux

$$f(x) \equiv 0 \pmod{p}, \qquad F(x) \equiv 0 \pmod{p}.$$

Si donc la seconde de ces deux congruences avait moins de ν racines de la forme A, il faudrait que la première eût plus de $p^\nu - \nu$ racines de la même forme, ce qui est impossible, puisqu'elle n'est que du degré $p^\nu - \nu$.

Ainsi l'on peut considérer une congruence irréductible de degré ν, suivant un module premier, comme ayant ν racines imaginaires qui sont des fonctions entières de l'une d'entre elles.

De la congruence $x^{p^\nu} - x \equiv 0 \pmod{p}$.

Il résulte de ce qui précède que s'il existe une congruence irréductible du degré ν, suivant le module premier p, et que i désigne une racine de cette congruence irréductible, la congruence

$$x^{p^\nu} - x = 0 \pmod{p}$$

admet p^ν racines qui sont toutes des fonctions entières de i. Or on peut prouver aisément l'existence d'une congruence irréductible de degré ν, quel que soit le module

premier p (*). Nous commencerons par établir le lemme suivant dont nous ferons usage.

Lemme. — *Soient $f(x)$ une fonction entière, p un nombre premier et n un nombre entier quelconque; on a*

$$f\left(x^{p^n}\right) = [f(x)]^{p^n} + p\chi(x),$$

$\chi(x)$ désignant une fonction entière.

Soit

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m;$$

la puissance $p^{\text{ième}}$ de $f(x)$ renfermera d'abord les puissances $p^{\text{ièmes}}$ des différents termes; elle renfermera, en outre, d'autres termes contenant certaines puissances de plusieurs termes de $f(x)$; le coefficient de l'un quelconque de ces derniers termes aura la forme

$$\frac{1.2\ldots p}{(1.2\ldots q_1)\ldots(1.2\ldots q_k)},$$

$q_1, q_2, \ldots, q_k$ étant des nombres inférieurs à p, ce coefficient est donc divisible par p et l'on a

$$[f(x)]^p + p\chi(x) = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots + a_m^p x^{mp};$$

mais, par le théorème de Fermat, on a

$$a^p \equiv a \pmod{p};$$

donc

$$[f(x)]^p + p\chi(x) = a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_m x^{mp},$$

ou

$$f(x^p) = [f(x)]^p + p\chi(x),$$

$\chi(x)$ désignant une fonction entière.

(*) Galois n'a indiqué aucune démonstration satisfaisante de ce point capital. La démonstration que j'ai trouvée et que je présente ici, ne laisse rien à désirer, je pense, sous le rapport de la rigueur et de la clarté.

Si l'on met $x^{p^{n-1}}$ au lieu de x, il vient

$$f(x^{p^n}) = \left[f(x^{p^{n-1}})\right]^p + p\chi(x),$$

$\chi(x)$ étant ici une nouvelle fonction entière. Cela posé, admettons que l'on ait

$$f(x^{p^{n-1}}) = [f(x)]^{p^{n-1}} + p\chi(x);$$

en élevant cette égalité à la puissance p et ayant égard à la précédente, il vient

$$f(x^{p^n}) = [f(x)]^{p^n} + p\chi(x).$$

Donc, si cette dernière égalité a lieu pour une valeur de l'exposant n, elle a lieu pour la valeur immédiatement supérieure; d'ailleurs elle a été démontrée pour $n = 1$, donc elle est générale.

Ce lemme établi, considérons la congruence

$$(1) \qquad x^{p^\nu} - x \equiv 0 \pmod{p},$$

et décomposons le premier membre en facteurs irréductibles, de manière que l'on ait

$$(2) \qquad F(x)F_1(x)F_2(x)\ldots = x^{p^\nu} - x + p\chi(x),$$

F, F_1,... et χ étant des fonctions entières. Parmi les facteurs $F(x)$, $F_1(x)$, etc., il y en a p qui sont du premier degré et qui ont respectivement pour valeurs

$$x,\ x-1,\ x-2,\ldots,\ x-p+1;$$

les autres facteurs sont de degrés supérieurs et deux quelconques d'entre eux ne sauraient être égaux, puisque la fonction $x^{p^\nu} - x$ n'a aucun facteur commun avec sa dérivée. En outre, la somme des degrés des polynômes

$F(x)$, $F_1(x)$, etc., est nécessairement égale à p^ν, car le premier terme du produit de ces polynômes doit détruire le terme x^{p^ν}.

Cela posé, je dis que parmi les polynômes $F(x)$, $F_1(x)$, etc., il n'y en a aucun dont le degré soit supérieur à ν. En effet, supposons, s'il est possible, que le degré μ de $F(x)$ soit supérieur à ν, et désignons par i une racine de la congruence irréductible

$$F(x) \equiv 0 \pmod{p}.$$

Posons aussi

$$f(i) = a_0 + a_1 i + a_2 i^2 + \ldots + a_{\mu-1} i^{\mu-1}.$$

$F(x)$ étant un facteur de $x^{p^\nu} - x + p\chi(x)$, la congruence (1) admet i pour racine, et l'on a

$$i^{p^\nu} \equiv i \pmod{p}.$$

Or, d'après le lemme qui précède, on a

$$[f(i)]^{p^\nu} \equiv f\left(i^{p^\nu}\right) \pmod{p};$$

donc

$$[f(i)]^{p^\nu} - f(i) \equiv 0 \pmod{p},$$

et, par suite, $f(i)$ est racine de la congruence (1). Nous sommes ainsi conduits à cette conséquence, que la congruence (1) qui est du degré p^ν aurait pour racines les p^μ valeurs distinctes dont $f(i)$ est susceptible : or cela est impossible si μ est $> \nu$; il est donc absurde de supposer que le degré de $F(x)$ soit supérieur à ν.

Je dis, en second lieu, que, parmi les polynômes $F(x)$, $F_1(x)$, etc., il y en a nécessairement quelques-uns dont le degré est égal à ν. En effet, si tous ces polynômes

sont de degré inférieur à ν, comme ils sont irréductibles, chacun d'eux divisera, suivant le module p, l'une des fonctions

$$x^p - x,\quad x^{p^2} - x,\quad x^{p^3} - x,\quad x^{p^{\nu-1}} - x,$$

en sorte que, si l'on décompose en facteurs irréductibles le produit de ces binômes, tous les polynômes $F(x)$, $F_1(x)$, etc., feront partie de ces facteurs. On aura donc

$$\begin{aligned}&(x^p - x)(x^{p^2} - x)\ldots(x^{p^{\nu-1}} - x)\\ &\quad = (x^{p^\nu} - x)\varphi(x) + p\chi(x),\end{aligned}$$

φ et χ étant des fonctions entières. Or une pareille égalité est impossible; en effet, les coefficients de $\varphi(x)$ étant rabaissés au-dessous de p, le premier terme du premier membre qui est du degré $p + p^2 + \ldots + p^{\nu-1}$ sera égal au premier terme de $(x^{p^\nu} - x)\varphi(x)$, dont le degré est au moins égal à p^ν; on aurait donc

$$p + p^2 + \ldots + p^{\nu-1} = \frac{p^\nu - p}{p-1} = \text{ou} > p^\nu,$$

ce qui est absurde.

On peut conclure de là qu'il existe, dans tous les degrés, des congruences irréductibles, suivant un module premier p, et, par suite, que la congruence

$$x^{p^\nu} - x \equiv 0 \pmod{p}$$

a p^ν racines qui dépendent nécessairement d'une seule congruence irréductible de degré ν.

Maintenant, pour avoir cette congruence irréductible, d'où dépendent les racines de la congruence

$$x^{p^\nu} - x \equiv 0 \pmod{p},$$

la méthode la plus générale sera de délivrer d'abord cette congruence de tous les facteurs communs qu'elle pourrait avoir avec des congruences de degré inférieur et de la forme $x^{p^\mu} - x \equiv 0$. On obtiendra ainsi une congruence qui devra se partager en congruences irréductibles de degré ν.

Propriété des racines d'une congruence irréductible.

On peut exprimer toutes les racines de la congruence irréductible de degré ν

$$F(x) \equiv 0 \pmod{p},$$

par les puissances de l'une quelconque d'entre elles.

En effet, nous avons vu que l'on a

$$F\left(x^{p^n}\right) = [F(x)]^{p^n} + p\chi(x),$$

χ étant une fonction entière. Si donc x désigne une racine de la proposée, toutes les racines seront représentées par

$$x,\quad x^p,\quad x^{p^2},\ldots,\quad x^{p^{\nu-1}}.$$

Toutefois, pour légitimer cette conclusion, il faut prouver que les quantités précédentes sont différentes. Il suffit pour cela de faire voir que si i désigne une racine de la proposée, on ne peut avoir

$$i^{p^{n+n'}} \equiv i^{p^{n'}},\quad \text{ou}\quad i^{p^{n'}}\left[i^{p^{n'}(p^n-1)} - 1\right] \equiv 0 \pmod{p}.$$

En effet, supposons que cela ait lieu. Comme $i^{p^{n'}}$ n'est pas nul, suivant le module p, on a

$$i^{p^{n'}(p^n-1)} - 1 \equiv 0 \pmod{p}.$$

Or l'exposant de la plus petite puissance de i congrue à l'unité, divise $p^\nu - 1$, et n'a, par suite, aucun facteur commun avec $p^{n'}$; on a donc

$$i^{p^n - 1} - 1 \equiv 0 \pmod{p},$$

ou

$$F(i) f(i) = i^{p^n - 1} - 1 + p\chi(i),$$

f et χ désignant des fonctions entières. Or cette égalité est impossible; car n étant inférieur à ν, $i^{p^n - 1} - 1$ ne peut admettre un diviseur irréductible $F(i)$ de degré ν. Donc on ne peut supposer $i^{p^{n+n'}} \equiv i^{p^{n'}}$.

Des racines primitives.

Considérons la congruence binôme

$$(1) \qquad x^{p^\nu - 1} - 1 \equiv 0 \pmod{p},$$

et soit i une racine d'une congruence irréductible de degré ν,

$$F(i) \equiv 0 \pmod{p}.$$

Si l'on fait

$$\alpha = a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

a_0, a_1, etc., étant des entiers inférieurs à p, on a, comme nous l'avons vu plus haut,

$$\alpha^n \equiv 1 \pmod{p},$$

n étant un diviseur de $p^\nu - 1$. Cela posé, si n est le plus petit nombre qui soit tel, que l'on ait

$$\alpha^n \equiv 1 \pmod{p},$$

nous dirons que α est une racine primitive de la congruence

(2) $$x^n - 1 \equiv 0 \pmod{p}.$$

Le premier membre de la congruence (1) est toujours divisible par le premier membre de la congruence (2), si n est un diviseur de $p^\nu - 1$; donc la congruence (2) a n racines qui sont des fonctions entières de i; nous allons montrer que, parmi ces n racines, il y en a toujours de primitives. Remarquons d'abord que les racines communes à deux congruences

$$x^n - 1 \equiv 0, \quad x^{n'} - 1 \equiv 0 \pmod{p},$$

dont les degrés n et n' divisent $p^\nu - 1$, appartiennent aussi à la congruence

$$x^\theta - 1 \equiv 0 \pmod{p},$$

où θ désigne le plus grand commun diviseur de n et n'. En effet, soient α une racine commune aux deux congruences proposées, et k le plus petit nombre, tel que l'on ait

$$\alpha^k \equiv 1 \pmod{p}.$$

Les puissances de α congrues à l'unité sont α^k, α^{2k}, etc., d'où il suit que k divise n et n'; il divise donc leur plus grand commun diviseur θ, et par conséquent α satisfait à

$$x^\theta - 1 \equiv 0 \pmod{p}.$$

On conclut de ce qui précède que les racines non primitives de la congruence

$$x^n - 1 \equiv 0 \pmod{p},$$

appartiennent à une deuxième congruence

$$x^\theta - 1 \equiv 0 \pmod{p},$$

dont le degré θ est un diviseur de n.

Supposons d'abord que n ne renferme qu'un seul facteur premier q, que l'on ait, par exemple,

$$n = q^\mu.$$

Les racines non primitives de la congruence

$$x^{q^\mu} - 1 \equiv 0 \pmod{p}$$

appartiendront aussi à

$$x^{q^{\mu-1}} - 1 \equiv 0 \pmod{p}.$$

Celle-ci a $q^{\mu-1}$ racines; donc la proposée a $q^\mu - q^{\mu-1}$, ou $q^\mu\left(1 - \frac{1}{q}\right)$ racines primitives.

Supposons, en second lieu, que n contienne plusieurs facteurs premiers, q, q', q'', etc., et soit

$$n = q^\mu q'^{\mu'} q''^{\mu''} \ldots;$$

la congruence proposée sera

$$x^{q^\mu q'^{\mu'} q''^{\mu''} \ldots} - 1 \equiv 0 \pmod{p}.$$

Considérons les congruences

$$x^{q^\mu} - 1 \equiv 0, \quad x^{q'^{\mu'}} - 1 \equiv 0, \ldots, \pmod{p};$$

et désignons par α une racine de la première, par α' une racine de la deuxième, etc. Le produit

$$\alpha\alpha' \ldots$$

sera une racine de la proposée, et ce sera même une racine primitive, si l'on prend pour α, α', etc., des racines primitives des congruences auxquelles elles appartiennent respectivement. Il suffit, pour établir cette proposition, de répéter textuellement des raisonnements que nous avons suffisamment développés dans la leçon précédente. On voit aussi que le nombre des racines primitives de la proposée est

$$q^{\mu} q'^{\mu'} q''^{\mu''} \ldots \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{q'}\right) \left(1 - \frac{1}{q''}\right) \ldots$$

Si α désigne une racine primitive de la congruence

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod{p},$$

toutes les racines de cette congruence seront représentées par

$$\alpha,\ \alpha^2,\ \alpha^3, \ldots,\ \alpha^{p^\nu - 1}.$$

Je dis, en outre, que α dépend d'une congruence irréductible de degré ν. En effet, le binôme $x^{p^\nu - 1} - 1$ n'admet aucun facteur irréductible de degré supérieur à ν; et, si α était racine d'une congruence irréductible de degré inférieur à ν, il n'y aurait pas $p^\nu - 1$ fonctions entières de α distinctes entre elles et différentes de zéro; par conséquent, les $p^\nu - 1$ premières puissances de α ne seraient pas distinctes, et alors α ne serait pas, comme on l'a supposé, une racine primitive. La congruence irréductible dont α dépend a pour racines

$$\alpha,\ \alpha^p,\ \alpha^{p^2}, \ldots,\ \alpha^{p^{\nu-1}},$$

comme on l'a vu plus haut, et l'on a

$$\alpha^{p^\nu} \equiv \alpha \pmod{p}.$$

Comme les puissances de p sont premières avec $p^{\nu} - 1$, on conclut aisément de là que toutes les racines de la congruence en α sont des racines primitives; par conséquent, le nombre total des racines primitives de la congruence

$$x^{p^{\nu}-1} - 1 \equiv 0 \pmod{p},$$

est un multiple de ν.

Recherche de toutes les racines d'une congruence quelconque.

Le principal avantage de la nouvelle théorie que nous avons exposée est, dit Galois, de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans leur degré.

La méthode pour avoir toutes ces racines sera très-simple. Premièrement, on pourra toujours préparer la congruence donnée $F(x) \equiv 0 \pmod{p}$, de manière qu'elle n'ait plus de racines égales, ou, en d'autres termes, de manière que le premier membre n'ait plus de facteur commun avec sa dérivée; et le moyen de le faire est évidemment le même que pour les équations ordinaires.

Ensuite, pour avoir les solutions entières, il suffira (vingt-troisième leçon) de chercher le plus grand commun diviseur à $F(x)$ et à $x^{p-1} - 1$.

Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand commun diviseur à $F(x)$ et à $x^{p^2-1} - 1$, et, en général, les solutions de l'ordre ν seront données par le plus grand commun diviseur à $F(x)$ et à $x^{p^{\nu}-1} - 1$.

Il est aisé de voir que si

$$F(x) \equiv 0 \pmod{p}$$

est une congruence quelconque de degré m, ses m racines peuvent s'exprimer toutes par des fonctions entières d'une seule racine i d'une congruence irréductible. En effet, décomposons le premier membre de la congruence proposée en facteurs irréductibles, et soit

$$F_1(x)\,F_2(x)\,F_3(x)\ldots = F(x) + p\chi(x),$$

χ étant une fonction entière. Soient ν, μ, λ, etc., les nombres inégaux par lesquels on peut exprimer les degrés des polynômes F_1, F_2, F_3, etc.; les racines de la congruence proposée appartiendront à l'une des congruences

$$x^{p^\nu} - x \equiv 0, \quad x^{p^\mu} - x \equiv 0, \quad x^{p^\lambda} - x \equiv 0, \ldots \quad (\text{mod. } p).$$

et, par suite, à la congruence

$$x^{p^{\nu\mu\lambda\ldots}} - x \equiv 0 \quad (\text{mod. } p).$$

Or, toutes les racines de cette dernière peuvent s'exprimer par une seule racine d'une congruence irréductible; donc la proposée aura la même propriété.

Application de la théorie à un exemple.

Pour donner un exemple de la théorie que nous venons de développer, considérons la congruence

$$x^{7^3-1} - 1 \equiv 0 \quad (\text{mod. } 7).$$

D'abord, il est facile ici d'obtenir une congruence irréductible du troisième degré. Effectivement, si h n'est pas résidu cubique de 7, la congruence

$$x^3 \equiv h \quad (\text{mod. } 7)$$

n'admettra aucune racine entière, et, par suite, elle

sera irréductible. Or, parmi les nombres 1, 2, 3, 4, 5, 6, il n'y a que 1 et 6 qui soient résidus cubiques de 7; donc les congruences

$$x^3 \equiv 2, \quad x^3 \equiv 3, \quad x^3 \equiv 4, \quad x^3 \equiv 5 \pmod{7}$$

sont irréductibles. Nous désignerons par i une racine de la congruence

$$i^3 \equiv 2 \pmod{7},$$

et alors les racines de la proposée auront toutes la forme

$$a_0 + a_1 i + a_2 i^2.$$

Cherchons maintenant une racine primitive de la congruence proposée qui est

$$(1) \qquad x^{342} - 1 \equiv 0 \quad \text{ou} \quad x^{2.3^2.19} - 1 \equiv 0 \pmod{7}.$$

Il suffit pour cela d'avoir une racine primitive de chacune des trois suivantes :

$$(2) \quad x^2 - 1 \equiv 0, \quad x^{3^2} - 1 \equiv 0, \quad x^{19} - 1 \equiv 0 \pmod{7}.$$

La racine primitive de la première des congruences (2) est -1; la deuxième de ces congruences (2) peut se mettre sous la forme

$$(x^3 - 1)(x^3 - 2)(x^3 - 4) \equiv 0 \pmod{7},$$

et ses racines primitives sont les racines des deux congruences

$$x^3 \equiv 2, \quad x^3 \equiv 4 \pmod{7};$$

donc i est une racine primitive de la deuxième des congruences (2). Il ne reste qu'à trouver une racine de $x^{19} - 1 \equiv 0$, ou plutôt de

$$\frac{x^{19} - 1}{x - 1} \equiv 0 \pmod{7}.$$

Essayons pour cela si l'on ne peut pas satisfaire à la question en posant simplement $x = a_0 + a_1 i$, au lieu de $a_0 + a_1 i + a_2 i^2$; nous devrons avoir

$$(a_0 + a_1 i)^{19} \equiv 1 \pmod{7},$$

ce qui, en développant par la formule de Newton et réduisant les puissances de a_0, a_1 et i par les formules

$$a_0^{6m} \equiv 1, \quad a_1^{6m} \equiv 1, \quad i^3 \equiv 2 \pmod{7},$$

se réduit à

$$3[a_0 - a_0^4 a_1^3 + (a_0^5 a_1^2 + a_0^2 a_1^5) i^2] \equiv 1,$$

d'où, en séparant,

$$3a_0 - 3a_0^4 a_1^3 \equiv 1, \quad a_0^5 a_1^2 + a_0^2 a_1^5 \equiv 0.$$

Ces deux dernières conditions sont satisfaites en posant

$$a_0 = -1, \quad a_1 = 1.$$

Donc $-1 + i$ est une racine primitive de la troisième des congruences (2). Le produit des trois quantités -1, i et $-1 + i$, qui est

$$i - i^2,$$

sera donc une racine primitive de la congruence proposée

$$x^{7^3-1} - 1 \equiv 0 \pmod{7};$$

par conséquent, cette expression jouit de la propriété qu'en l'élevant à toutes les puissances, on obtiendra $7^3 - 1$ expressions différentes et de la forme

$$a_0 + a_1 i + a_2 i^2.$$

Si l'on veut connaître la congruence irréductible dont dépend la racine primitive que nous venons de trouver, il

24

faudra éliminer i entre

$$\alpha = i - i^2 \quad \text{et} \quad i^3 \equiv 2 \pmod{7}.$$

En élevant la valeur de α au cube, puis réduisant les exposants de i, il vient

$$\alpha^3 \equiv -2 + i - i^2 \pmod{7};$$

d'où

$$\alpha^3 - \alpha + 2 \equiv 0 \pmod{7}.$$

Il sera convenable de prendre pour *base* des imaginaires et de représenter par i la racine de cette congruence, en sorte que l'on aura

$$i^3 - i + 2 \equiv 0 \pmod{7},$$

et l'on obtiendra toutes les imaginaires de la forme

$$a_0 + a_1 i + a_2 i^2$$

en élevant i à toutes les puissances et réduisant par la précédente congruence.

VINGT-SIXIÈME LEÇON.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre.

Nous avons démontré, dans la vingt-deuxième leçon, l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième. Mais une équation de degré quelconque, dont les coefficients ont des valeurs particulières déterminées, peut, dans certains cas, être résolue algébriquement (*). Ainsi, les équations auxquelles conduit le problème de la division du cercle en un nombre premier p de parties égales sont toujours résolubles par radicaux; et, comme M. Gauss l'a établi dans ses Recherches arithmétiques, chacun des radicaux dont l'expression des racines est composée, a pour indice l'un des facteurs premiers de $p - 1$. Ces équations ont cette propriété, que chaque racine peut s'exprimer rationnellement par l'une quelconque des autres (*voyez* treizième leçon); Abel, en partant de cette remarque, a fait voir que, si deux racines d'une équation irréductible sont tellement liées entre elles, que l'une puisse s'exprimer ra-

(*) L'équation du neuvième degré dont dépend la recherche des points d'inflexion des courbes du troisième degré est toujours résoluble algébriquement (*voir* la Note XII).

Galois a donné la condition nécessaire et suffisante pour qu'une équation irréductible de degré premier soit résoluble par radicaux (*voir* le Journal de M. Liouville, tome XI). Dans ces derniers temps, un géomètre allemand, M. Léopold Kronecker, s'est occupé avec le plus grand succès de la résolution des équations algébriques. On trouvera dans la Note XIII la traduction du résumé que M. Kronecker a fait lui-même de ses recherches.

tionnellement par l'autre, on peut toujours ramener la résolution de l'équation à celle d'équations de degrés moindres. Il y a même des cas où l'équation est résoluble algébriquement; cela arrive en particulier si son degré est un nombre premier.

Nous allons exposer ici ces recherches d'Abel, et nous ferons ensuite l'application de sa méthode aux équations dont dépend la division du cercle en un nombre premier de parties égales.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre.

Lemme. — *Si $f(x) = 0$ est une équation irréductible, $F(x)$ une fonction rationnelle, et que l'équation $F(x) = 0$ admette une racine x_1 de $f(x) = 0$, elle admettra aussi toutes les autres.*

Soit, en effet,

$$F(x) = \frac{\varphi(x)}{\psi(x)},$$

φ et ψ désignant des fonctions entières; la racine x_1 sera, par hypothèse, commune aux équations

$$f(x) = 0, \quad \varphi(x) = 0;$$

et cela exige que le polynôme $\varphi(x)$ soit divisible par $f(x)$, car autrement il y aurait un diviseur commun à ces polynômes, et l'équation $f(x) = 0$ ne serait pas irréductible. Soit donc

$$\varphi(x) = f(x)\,\varpi(x),$$

on aura

$$F(x) = \frac{\varpi(x)}{\psi(x)} f(x),$$

et, par conséquent, l'équation $F(x) = 0$ admettra toutes les racines de $f(x) = 0$.

Soit maintenant

$$(1) \qquad f(x) = 0$$

une équation irréductible de degré μ, et supposons que deux racines x' et x_1 soient liées entre elles par l'équation

$$x' = \theta x_1,$$

où θx désigne une fonction rationnelle de x et de quantités connues. x' étant racine de l'équation (1), on aura

$$f(\theta x_1) = 0;$$

d'où il suit que x_1 sera racine de l'équation

$$(2) \qquad f(\theta x) = 0,$$

et, par conséquent, cette équation (2) admettra toutes les racines de l'équation (1), car celle-ci est irréductible, et $f(\theta x)$ est une fonction rationnelle. En d'autres termes, si x désigne une racine quelconque de l'équation (1), θx sera aussi racine de cette équation. Mais θx_1 est racine de l'équation (1); donc $\theta\theta x_1$ le sera aussi, ainsi que $\theta\theta\theta x_1$, et généralement, en répétant sur x_1 un nombre quelconque de fois l'opération désignée par θ, on obtiendra toujours une racine de l'équation (1).

Soit, pour abréger,

$$\theta\theta x_1 = \theta^2 x_1, \quad \theta\theta^2 x_1 = \theta^3 x_1, \quad \theta\theta^3 x_1 = \theta^4 x_1, \ldots,$$

tous les termes de la série

$$(3) \qquad x_1, \; \theta x_1, \; \theta^2 x_1, \; \theta^3 x_1, \ldots$$

seront des racines de l'équation (1). Mais la série (3) renferme une infinité de termes, tandis que l'équation (1) n'a que μ racines; il faut donc que quelques-unes des quantités (3) se trouvent répétées un nombre infini de fois.

Supposons, par exemple, que l'on ait

$$\theta^{m+n} x_1 = \theta^m x_1,$$

ou

$$\theta^n(\theta^m x_1) - \theta^m x_1 = 0,$$

l'équation

$$\theta^n x - x = 0$$

a la racine $\theta^m x_1$ commune avec l'équation (1); elle admettra donc toutes les racines de l'équation (1), et l'on aura

$$\theta^n x_1 - x_1 = 0,$$

ou

$$\theta^n x_1 = x_1.$$

On tire de là

$$\theta^{n+k} x_1 = \theta^k x_1;$$

d'où il suit qu'à partir du $n^{ième}$, les termes de la série (3) se reproduiront dans le même ordre, et que cette série ne contiendra que ces n quantités distinctes

$$(4) \qquad x_1, \quad \theta x_1, \quad \theta^2 x_1, \quad \ldots, \quad \theta^{n-1} x_1.$$

Ces n quantités seront, en effet, distinctes, si n est le nombre de fois qu'il faut répéter sur x_1 l'opération désignée par θ pour reproduire x_1.

Si l'on a $\mu = n$, la série (4) contient toutes les racines de l'équation (1); ce cas est celui de l'équation

$$\frac{x^{n+1} - 1}{x - 1} = 0,$$

où $n + 1$ est un nombre premier (*), ainsi que nous l'avons établi dans la vingt-quatrième leçon.

Supposons $\mu > n$, et soit x_2 une racine de l'équation (1) qui ne fasse pas partie de la série (4); on fera voir, comme précédemment, que toutes les quantités

$$(5) \qquad x_2, \quad \theta x_2, \quad \theta^2 x_2, \ldots, \quad \theta^{n-1} x_2, \ldots$$

sont également racines de l'équation (1). Or je dis que,

(*) L'équation dont il s'agit ici est irréductible. On trouvera la démonstration de cette importante propriété dans la Note IX.

dans la série (5), les n premiers termes

(6) $$x_2,\quad \theta x_2,\quad \theta^2 x_2,\ldots,\quad \theta^{n-1} x_2$$

sont les seuls qui puissent être différents. En effet, l'équation

$$\theta^n x - x = 0$$

admet la racine x_1 de l'équation (1); donc elle admettra toutes les autres, et l'on aura

$$\theta^n x_2 = x_2,$$

d'où

$$\theta^{n+k} x_2 = \theta^k x_2.$$

Par conséquent, les termes de la série (5) se reproduiront dans le même ordre, à partir du $n^{ième}$, et, parmi ces termes, les seuls qui puissent être distincts sont renfermés dans la série (6).

Je dis maintenant que les termes de la série (6) sont effectivement différents entre eux, et distincts des quantités (4).

L'égalité

$$\theta^k x_2 = \theta^i x_2,$$

où k et i sont inférieurs à n, est effectivement impossible; car, d'après le lemme établi au commencement de cette leçon, elle entraînerait

$$\theta^k x_1 = \theta^i x_1,$$

ce qui n'a pas lieu, puisque les quantités (4) sont différentes.

L'égalité

$$\theta^k x_2 = \theta^i x_1$$

est de même impossible. Si, en effet, elle avait lieu, il en résulterait

$$\theta^{n-k}\theta^i x_1 = \theta^{n-k}\theta^k x_2,$$

ou

$$\theta^{n-k+i} x_1 = \theta^n x_2 = x_2,$$

et, par conséquent, x_2 ferait partie de la série (4), ce qui est contre l'hypothèse.

Le nombre des racines de l'équation (1) renfermées dans les séries (4) et (6) est $2n$; on a donc nécessairement $\mu = 2n$ ou $\mu > 2n$.

Supposons $\mu > 2n$, et désignons par x_3 une racine de l'équation (1) qui ne fasse pas partie des groupes (4) et (6); en raisonnant comme précédemment, on formera un troisième groupe de n racines

$$x_3,\quad \theta x_3,\quad \theta^2 x_3,\ldots,\quad \theta^{n-1} x_3,$$

toutes distinctes et différentes des quantités (4) et (6); d'où il suit nécessairement que l'on a $\mu = 3n$ ou $\mu > 3n$.

En continuant ainsi, on verra que les μ racines de l'équation (1) peuvent être partagées en un certain nombre m de groupes composés chacun de n termes, en sorte que

$$\mu = mn.$$

Les racines de l'équation (1) seront alors

$$(7)\qquad \left\{\begin{array}{llll} x_1, & \theta x_1, & \theta^2 x_1,\ldots, & \theta^{n-1} x_1,\\ x_2, & \theta x_2, & \theta^2 x_2,\ldots, & \theta^{n-1} x_2,\\ x_3, & \theta x_3, & \theta^2 x_3,\ldots, & \theta^{n-1} x_3,\\ \ldots & \ldots & \ldots & \ldots\\ \ldots & \ldots & \ldots & \ldots\\ x_m, & \theta x_m, & \theta^2 x_m,\ldots, & \theta^{n-1} x_m. \end{array}\right.$$

Considérons l'équation de degré n qui a pour racines les racines de l'un de ces groupes, du premier par exemple, et soit

$$(x - x_1)(x - \theta x_1)(x - \theta^2 x_1)\ldots(x - \theta^{n-1} x_1) = 0,$$

ou

$$(8)\qquad x^n + A'_1 x^{n-1} + A'_2 x^{n-2} + \ldots + A'_{n-1} x + A'_n = 0$$

cette équation. Les coefficients

$$A'_1,\quad A'_2,\ldots,\quad A'_n$$

sont des fonctions rationnelles et symétriques des quantités

$$x_1,\quad \theta x_1,\quad \theta^2 x_1,\ldots,\quad \theta^{n-1} x_1,$$

et ne dépendent, comme on va voir, que d'une seule équation du degré m.

Soit, en effet, y_1 une fonction rationnelle et symétrique quelconque des quantités

(9) $$x_1,\quad \theta x_1,\quad \theta^2 x_1,\ldots,\quad \theta^{n-1} x_1;$$

θx_1, $\theta^2 x_1$, etc., étant des fonctions rationnelles de x_1, y_1 le sera aussi, et nous poserons

$$y_1 = F(x_1),$$

F désignant une fonction rationnelle. En outre, à cause de $\theta^n x_1 = x_1$, les quantités (9) ne feront que se changer les unes dans les autres si l'on remplace x_1 par θx_1, $\theta^2 x_1,\ldots, \theta^{n-1} x_1$; et comme y_1 est une fonction symétrique de ces quantités, sa valeur sera invariable par ces changements; on aura donc

$$y_1 = F(x_1) = F(\theta x_1) = F(\theta^2 x_1) = \ldots = F(\theta^{n-1} x_1).$$

Désignons par

$$y_2,\quad y_3,\ldots,\quad y_m$$

les valeurs que prend y_1 quand on y remplace x_1 successivement par

$$x_2,\quad x_3,\ldots,\quad x_m,$$

on aura

$$y_2 = F(x_2) = F(\theta x_2) = F(\theta^2 x_2) = \ldots = F(\theta^{n-1} x_2),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_m = F(x_m) = F(\theta x_m) = F(\theta^2 x_m) = \ldots = F(\theta^{n-1} x_m).$$

Soit maintenant

$$(y-y_1)(y-y_2)\ldots(y-y_m)=0,$$

ou

$$(10)\quad y^m+p_1y^{m-1}+p_2y^{m-2}+\ldots+p_{m-1}y+p_m=0$$

l'équation qui a pour racines $y_1, y_2,\ldots, y_m$; je dis que les coefficients p_1, p_2, etc., de cette équation peuvent être exprimés rationnellement par les coefficients de l'équation proposée (1). On a, en effet, quel que soit l'entier λ,

$$y_1^\lambda=\frac{1}{n}\left\{[\mathrm{F}(x_1)]^\lambda+[\mathrm{F}(\theta x_1)]^\lambda+\ldots+[\mathrm{F}(\theta^{n-1}x_1)]^\lambda\right\},$$

$$y_2^\lambda=\frac{1}{n}\left\{[\mathrm{F}(x_2)]^\lambda+[\mathrm{F}(\theta x_2)]^\lambda+\ldots+[\mathrm{F}(\theta^{n-1}x_2)]^\lambda\right\},$$

....

....

$$y_m^\lambda=\frac{1}{n}\left\{[\mathrm{F}(x_m)]^\lambda+[\mathrm{F}(\theta x_m)]^\lambda+\ldots+[\mathrm{F}(\theta^{n-1}x_m)]^\lambda\right\},$$

et, en ajoutant,

$$y_1^\lambda+y_2^\lambda+\ldots+y_m^\lambda=\frac{1}{n}\sum[\mathrm{F}(x)]^\lambda.$$

Le signe $\sum$ du second membre s'étend à toutes les racines de l'équation proposée; ce second membre est donc une fonction symétrique et rationnelle de toutes les racines; d'où il résulte que les sommes de puissances semblables des racines de l'équation (10) peuvent être exprimées rationnellement par les coefficients de l'équation proposée. On pourra donc aussi exprimer de la même manière les coefficients p_1, p_2, etc., comme nous l'avions annoncé.

La fonction rationnelle et symétrique y_1 des quantités (9), qui peut d'ailleurs être choisie à volonté, dépend donc directement d'une équation de degré m. D'ailleurs

les fonctions

$$y_1,\ A'_1,\ A'_2,\ldots,\ A'_n$$

sont des fonctions semblables; car elles peuvent toutes être considérées comme des fonctions rationnelles de la seule racine x_1. On pourra donc exprimer

$$A'_1,\ A'_2,\ldots,\ A'_n$$

en fonction rationnelle de y_1.

Nous sommes ainsi conduits à l'une des applications les plus importantes de la théorie des fonctions semblables, que nous avons développée dans une précédente leçon; mais, comme cette théorie est sujette à quelques cas d'exception, il ne sera pas inutile d'entrer, avec Abel, dans le détail du calcul des coefficients A'_1, A'_2, etc.

Désignons par $\psi(x_1)$ l'un quelconque de ces coefficients; ψ est une fonction rationnelle qui ne doit pas changer quand on remplace x_1 par $\theta x_1, \theta^2 x_1,\ldots, \theta^{n-1} x_1$, puisque $\psi(x_1)$ est, comme y_1, une fonction symétrique des quantités (9); et il en sera de même de la fonction

$$y_1^\lambda \psi(x_1), \quad \text{ou} \quad [F(x_1)]^\lambda \psi(x_1).$$

On aura donc

$$y_1^\lambda \psi(x_1) = \frac{1}{n}\left\{\begin{array}{l} [F(x_1)]^\lambda \psi(x_1) + [F(\theta x_1)]^\lambda \psi(\theta x_1) + \ldots \\ + [F(\theta^{n-1} x_1)]^\lambda \psi(\theta^{n-1} x_1) \end{array}\right\};$$

en remplaçant x_1 successivement par $x_2, x_3,\ldots, x_m$, on aura des expressions semblables pour $y_2^\lambda \psi(x_2),\ldots,$ $y_m^\lambda \psi(x_m)$; et, si l'on pose

$$(11) \qquad t_\lambda = y_1^\lambda \psi(x_1) + y_2^\lambda \psi(x_2) + \ldots + y_m^\lambda \psi(x_m),$$

on aura

$$t_\lambda = \frac{1}{n} \sum [F(x)]^\lambda \psi(x),$$

le signe $\sum$ s'étendant à toutes les racines de l'équation (1).

On voit, par là, que t_λ est une fonction symétrique et rationnelle des racines de l'équation (1), qui pourra, par conséquent, s'exprimer rationnellement en fonction des quantités connues.

Cela posé, en prenant pour λ les valeurs 0, 1, 2, 3,..., $(m-1)$, l'équation (11) donnera les suivantes :

$$(12)\quad \left\{\begin{array}{l} \psi(x_1)+\psi(x_2)+\ldots+\psi(x_m)=t_0,\\ y_1\psi(x_1)+y_2\psi(x_2)+\ldots+y_m\psi(x_m)=t_1,\\ y_1^2\psi(x_1)+y_2^2\psi(x_2)+\ldots+y_m^2\psi(x_m)=t_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ y_1^{m-1}\psi(x_1)+y_2^{m-1}\psi(x_2)+\ldots+y_m^{m-1}\psi(x_m)=t_{m-1}, \end{array}\right.$$

dont les seconds membres peuvent être considérés comme connus.

Pour avoir la valeur de $\psi(x_1)$, ajoutons les équations (12) après les avoir respectivement multipliées par les indéterminées

$$R_0,\quad R_1,\ldots,\quad R_{m-2},\quad 1,$$

et faisons, pour abréger,

$$(13)\qquad \varphi(y)=y^{m-1}+R_{m-2}y^{m-2}+\ldots+R_1y+R_0,$$

on aura

$$\begin{aligned}\varphi(y_1)\psi(x_1)+\varphi(y_2)\psi(x_2)+\ldots+\varphi(y_m)\psi(x_m)\\ =t_0R_0+t_1R_1+\ldots+t_{m-2}R_{m-2}+t_{m-1};\end{aligned}$$

et, si l'on détermine les facteurs R_0, R_1, etc., par les conditions

$$\varphi(y_2)=0,\quad \varphi(y_3)=0,\ldots,\quad \varphi(y_m)=0,$$

on aura

$$(14)\qquad \psi(x_1) = \frac{t_0 R_0 + t_1 R_1 + \ldots + t_{m-2} R_{m-2} + t_{m-1}}{\varphi(y_1)}.$$

Cherchons maintenant les valeurs de R_0, R_1, etc. D'après notre hypothèse, l'équation

$$\varphi(y) = 0$$

doit avoir pour racines $y_2, y_3, \ldots, y_m$; mais ces racines appartiennent aussi à l'équation (10), qui admet en outre la racine y_1, on aura donc

$$(15)\quad \left\{ \begin{array}{l} \varphi(y) = \dfrac{y^m + p_1 y^{m-1} + p_2 y^{m-2} + \ldots + p_{m-1} y + p_m}{y - y_1} \\ \quad = y^{m-1} \left. \begin{array}{l} + p_1 \\ + y_1 \end{array} \right| y^{m-2} \left. \begin{array}{l} + p_2 \\ + p_1 y_1 \\ + y_1^2 \end{array} \right| y^{m-3} + \ldots + \begin{array}{l} p_{m-1} \\ + p_{m-2} y_1 \\ + \ldots\ldots \\ \ldots\ldots \\ + p_1 y_1^{m-2} \\ + y_1^{m-1}. \end{array} \end{array} \right.$$

Comparant les valeurs $\varphi(y)$ données par les équations (13) et (15), on trouve

$$(16)\qquad \left\{ \begin{array}{l} R_{m-2} = p_1 + y_1, \\ R_{m-3} = p_2 + p_1 y_1 + y_1^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ R_1 = p_{m-2} + p_{m-3} y_1 + \ldots + y_1^{m-2}, \\ R_0 = p_{m-1} + p_{m-2} y_1 + \ldots + y_1^{m-1}. \end{array} \right.$$

On tire aussi de l'équation (15)

$$\varphi(y_1) = m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \ldots + 2 p_{m-2} y_1 + p_{m-1},$$

et en faisant, pour abréger,

$$T_0 = t_0 p_{m-1} + t_1 p_{m-2} + \ldots + t_{m-2} p_1 + t_{m-1},$$
$$T_1 = t_0 p_{m-2} + t_1 p_{m-3} + \ldots + t_{m-2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$T_{m-2} = t_0 p_1 + t_1,$$
$$T_{m-1} = t_0,$$

on aura cette valeur de $\psi(x_1)$,

$$(17)\quad \psi(x_1) = \frac{T_{m-1} y_1^{m-1} + T_{m-2} y_1^{m-2} + \ldots + T_1 y_1 + T_0}{m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \ldots + 2 p_{m-2} y_1 + p_{m-1}}.$$

La formule précédente n'est en défaut que si le dénominateur du second membre est nul. Or, je dis qu'on peut toujours faire en sorte que cela ne soit pas. En effet, ce dénominateur est égal au produit

$$(y_1 - y_2)(y_1 - y_3) \ldots (y_1 - y_m),$$

et pour qu'il soit nul, il faut que l'un des facteurs le soit, que l'on ait, par exemple,

$$y_1 = y_k.$$

Cela posé, prenons pour y_1 la fonction

$$y_1 = (\alpha - x_1)(\alpha - \theta x_1)(\alpha - \theta^2 x_1) \ldots (\alpha - \theta^{n-1} x_1),$$

α étant indéterminé; l'équation $y_1 = y_k$, ou

$$(\alpha - x_1)(\alpha - \theta x_1) \ldots = (\alpha - x_k)(\alpha - \theta x_k) \ldots,$$

ne peut avoir lieu, quel que soit α, à moins d'être identique; ce qui est impossible, puisque les quantités x_k, θx_k, etc., sont différentes de x_1, θx_1, etc. D'où il suit qu'en choisissant y_1, comme il vient d'être dit, l'équation (17) donnera pour $\psi(x_1)$ une valeur finie et déterminée.

Les coefficients A'_1, A'_2, etc., de l'équation (8) peuvent

donc s'exprimer rationnellement par une même fonction y_1 dont la valeur dépend d'une équation du degré m; et si l'on remplace y_1 successivement par $y_2, y_3, \ldots, y_m$, on aura m équations du degré n, dont les racines seront respectivement

$$\begin{array}{l} x_1,\ \theta x_1, \ldots,\ \theta^{n-1} x_1, \\ x_2,\ \theta x_2, \ldots,\ \theta^{n-1} x_2, \\ \ldots\ldots\ldots\ldots\ \ldots\ldots \\ x_m,\ \theta x_m, \ldots,\ \theta^{n-1} x_m. \end{array}$$

D'où il suit que l'équation proposée peut être décomposée en m équations chacune du degré n, dont les coefficients sont respectivement des fonctions rationnelles d'une même racine d'une équation du degré m.

Cette dernière équation n'est pas en général résoluble algébriquement, quand son degré surpasse le quatrième; mais l'équation (8) et les autres semblables le sont toujours, en supposant connus les coefficients A'_1, A''_1, etc., comme nous le démontrerons dans la leçon suivante.

VINGT-SEPTIÈME LEÇON.

Résolution algébrique des équations dont toutes les racines peuvent être représentées par x, θx, $\theta^2 x, \ldots, \theta^{\mu-1} x$, θx étant une fonction rationnelle de x et de quantités connues, telle que $\theta^\mu x = x$. — Cas où les quantités connues de f et de θ sont réelles. — Première méthode particulière relative aux équations dont le degré est un nombre composé. — Deuxième méthode.

D'après la théorie exposée dans la leçon précédente, si deux racines d'une équation irréductible de degré $\mu = mn$ sont telles, que l'on puisse exprimer rationnellement l'une par l'autre, l'équation se décompose en m équations du degré n dont les racines peuvent être représentées par

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{n-1} x,$$

et dont les coefficients sont des fonctions rationnelles respectivement d'une même racine d'une équation de degré m.

Si l'on a $m = 1$, et par suite $\mu = n$, ce qui arrive nécessairement dans le cas de μ premier, les μ racines de l'équation proposée sont représentées par

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{\mu-1} x,$$

θx désignant une fonction rationnelle de x et de quantités connues, telle que

$$\theta^\mu x = x.$$

Toute équation qui a cette propriété peut être résolue algébriquement : la démonstration de cet important théorème va faire le sujet de cette leçon.

Résolution algébrique des équations dont toutes les racines peuvent être représentées par x, θx, $\theta^2 x$,...., $\theta^{\mu-1} x$, θx étant une fonction rationnelle de x et de quantités connues, telle que $\theta^\mu x = x$.

Soit

$$(1) \qquad f(x) = 0$$

une équation de degré μ, dont les racines sont

$$x,\ \theta x,\ \theta^2 x, \ldots,\ \theta^{\mu-1} x,$$

θx désignant une fonction rationnelle de x et de quantités connues, telle que l'on ait

$$(2) \qquad \theta^\mu x = x,$$

et, par conséquent,

$$(3) \qquad \theta^{\mu+k} x = \theta^k x.$$

Désignons par α une racine quelconque de l'équation

$$x^\mu = 1,$$

et posons, avec Lagrange (dix-huitième leçon),

$$(4) \quad \psi(x) = \left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x\right)^\mu;$$

je dis que la fonction $\psi(x)$ est exprimable rationnellement par les quantités connues de $f(x)$ et de $\theta(x)$.

En effet, remplaçons x par $\theta^m x$ dans l'équation (4), on aura

$$\psi(\theta^m x) = \left(\theta^m x + \alpha\theta^{m+1} x + \alpha^2\theta^{m+2} x + \ldots + \alpha^{\mu-1}\theta^{m+\mu-1} x\right)^\mu,$$

et, en ayant égard aux équations (2) et (3),

$$\psi(\theta^m x) = \left(\theta^m x + \alpha\theta^{m+1} x + \ldots + \alpha^{\mu-m} x + \alpha^{\mu-m+1}\theta x + \ldots + \alpha^{\mu-1}\theta^{m-1} x\right)^\mu$$

$$= \left(\alpha^{\mu-m} x + \alpha^{\mu-m+1}\theta x + \ldots + \alpha^{\mu-1}\theta^{m-1} x + \theta^m x + \ldots + \alpha^{\mu-m-1}\theta^{\mu-1} x\right)^\mu$$

$$= \left(\alpha^{\mu-m}\right)^\mu \left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x\right)^\mu,$$

ou enfin, à cause de $\alpha^\mu = 1$,

$$\psi(\theta^m x) = \psi(x).$$

Donnant à m les valeurs successives $0, 1, 2, \ldots, \mu - 1$, on a

$$\psi(x) = \psi(\theta x) = \psi(\theta^2 x) = \ldots = \psi(\theta^{\mu-1} x),$$

et, par conséquent,

$$\psi(x) = \frac{1}{\mu}\left[\psi(x) + \psi(\theta x) + \ldots + \psi(\theta^{\mu-1} x)\right];$$

d'où il suit que $\psi(x)$ est une fonction rationnelle et symétrique de toutes les racines de l'équation (1); elle pourra donc être exprimée rationnellement par les coefficients de cette équation.

Posons alors

$$\psi(x) = v,$$

on aura

$$x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v},$$

v étant une quantité connue. Et si l'on désigne par

$$1, \alpha_1, \alpha_2, \ldots, \alpha_{\mu-1}$$

les μ racines de l'équation

$$x^\mu = 1,$$

par

$$v_0, v_1, v_2, \ldots, v_{\mu-1}$$

les valeurs correspondantes de v, on aura

$$(5)\quad \left\{ \begin{array}{l} x + \theta x + \theta^2 x + \ldots\ldots\ldots\ldots + \theta^{\mu-1} x = \sqrt[\mu]{v_0}, \\ x + \alpha_1\theta x + \alpha_1^2\theta^2 x + \ldots\ldots + \alpha_1^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v_1}, \\ x + \alpha_2\theta x + \alpha_2^2\theta^2 x + \ldots\ldots + \alpha_2^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x + \alpha_{\mu-1}\theta x + \alpha_{\mu-1}^2\theta^2 x + \ldots + \alpha_{\mu-1}^{\mu-1}\theta^{\mu-1} x = \sqrt[\mu]{v_{\mu-1}}. \end{array} \right.$$

La quantité $\sqrt[\mu]{v_0}$ est immédiatement donnée par l'équation (1); car si l'on désigne par A le coefficient de $x^{\mu-1}$ dans cette équation, on a

$$\sqrt[\mu]{v_0} = -\text{A}.$$

En ajoutant les équations (5), et ayant égard aux propriétés connues des racines α, on a

$$(6) \qquad x = \frac{-\text{A} + \sqrt[\mu]{v_1} + \sqrt[\mu]{v_2} + \ldots + \sqrt[\mu]{v_{\mu-1}}}{\mu};$$

et l'on aura généralement la valeur d'une racine quelconque $\theta^m x$, en ajoutant les équations (5) respectivement multipliées par

$$1,\ \alpha_1^{-m},\ \alpha_2^{-m},\ \alpha_3^{-m},\ldots,\ \alpha_{\mu-1}^{-m};$$

on trouve ainsi

$$(7) \quad \theta^m x = \frac{-\text{A} + \alpha_1^{-m}\sqrt[\mu]{v_1} + \alpha_2^{-m}\sqrt[\mu]{v_2} + \ldots + \alpha_{\mu-1}^{-m}\sqrt[\mu]{v_{\mu-1}}}{\mu},$$

et l'on déduira de cette formule les valeurs de θx, $\theta^2 x,\ldots$, $\theta^{\mu-1} x$, en donnant à m les valeurs $1, 2, 3,\ldots, (\mu-1)$.

Dans l'équation (6) et dans toutes celles qu'on déduit de l'équation (7), on doit considérer chaque radical $\sqrt[\mu]{v_1}$, $\sqrt[\mu]{v_2},\ldots$, $\sqrt[\mu]{v_{\mu-1}}$, comme ayant toujours la même valeur. Si on laisse à chaque radical toute sa généralité, l'équation (7) ne diffère aucunement de l'équation (6), et cette dernière renferme l'expression de toutes les racines. Il y a même ici une difficulté, car l'équation (6) donne pour x une expression qui a $\mu^{\mu-1}$ valeurs, tandis

que l'équation (1) n'a que μ racines. Mais nous avons déjà eu l'occasion d'indiquer comment on peut faire disparaître cette ambiguïté, en remarquant que quand on a fixé la valeur de l'un des radicaux, les autres sont par cela même déterminés.

En effet, désignons par α une racine primitive de l'équation

$$\alpha^\mu = 1,$$

et posons

$$\alpha_1 = \alpha, \quad \alpha_2 = \alpha^2, \quad \alpha_3 = \alpha^3, \ldots, \quad \alpha_{\mu-1} = \alpha^{\mu-1},$$

on aura

$$\sqrt[\mu]{v_1} = x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x,$$

$$\sqrt[\mu]{v_n} = x + \alpha^n\theta x + \alpha^{2n}\theta^2 x + \ldots + \alpha^{(\mu-1)n}\theta^{\mu-1}x.$$

Si l'on change x en $\theta^m x$, $\sqrt[\mu]{v_1}$ n'éprouvera d'autre changement que d'être multiplié par $\alpha^{\mu-m}$; cela résulte immédiatement d'un calcul fait au commencement de cette leçon. Pareillement $\sqrt[\mu]{v_n}$ sera, par le même changement de x en $\theta^m x$, multiplié par $\alpha^{n(\mu-m)}$, d'où il suit que le produit

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n}$$

sera multiplié par $\alpha^{\mu(\mu-m)} = 1$, c'est-à-dire qu'il n'éprouvera aucun changement. Si donc on pose

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n} = \varphi(x),$$

on aura

$$\varphi(x) = \varphi(\theta x) = \varphi(\theta^2 x) = \ldots = \varphi(\theta^{\mu-1}x),$$

et, par conséquent,

$$\varphi(x) = \frac{1}{\mu}\left[\varphi(x) + \varphi(\theta x) + \ldots + \varphi(\theta^{\mu-1} x)\right].$$

$\varphi(x)$ est donc une fonction rationnelle et symétrique des racines de l'équation (1), et on pourra l'exprimer rationnellement par les quantités connues; en désignant par a_n sa valeur, on aura

$$\sqrt[\mu]{\nu_n}\left(\sqrt[\mu]{\nu_1}\right)^{\mu-n} = a_n,$$

ou

$$\sqrt[\mu]{\nu_n} = \frac{a_n}{\nu_1}\left(\sqrt[\mu]{\nu_1}\right)^n.$$

On pourra de cette manière exprimer chacun des radicaux $\sqrt[\mu]{\nu_2}$, $\sqrt[\mu]{\nu_3}$, etc., en fonction rationnelle de $\sqrt[\mu]{\nu_1}$, et l'équation (6) prendra la forme

$$(8)\quad x = \frac{1}{\mu}\left[-A + \sqrt[\mu]{\nu_1} + \frac{a_2}{\nu_1}\left(\sqrt[\mu]{\nu_1}\right)^2 + \frac{a_3}{\nu_1}\left(\sqrt[\mu]{\nu_1}\right)^3 + \ldots + \frac{a_{\mu-1}}{\nu_1}\left(\sqrt[\mu]{\nu_1}\right)^{\mu-1}\right].$$

Cette expression de x a précisément μ valeurs, et représente bien les μ racines de l'équation proposée.

Il résulte de ce qui précède que *si les μ racines d'une équation quelconque peuvent être représentées par*

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{\mu-1} x,$$

θx étant une fonction rationnelle telle que $\theta^\mu = x$, l'équation est toujours soluble par radicaux, ainsi que nous l'avions annoncé.

Et en rapprochant cet énoncé du théorème démontré dans la dernière leçon, on a cet autre théorème :

Si deux racines d'une équation irréductible de degré premier sont telles, que l'une puisse s'exprimer ration-

nellement en fonction de l'autre, l'équation est soluble par radicaux.

Cas où les quantités connues de f et de θ sont réelles.

Si tous les coefficients de f et de θ sont réels, on a un théorème remarquable, que M. Gauss a établi le premier pour les équations dont dépend la division du cercle en parties égales.

Nous avons posé précédemment

$$v_1 = \left(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x\right)^\mu,$$

et nous avons établi que v_1 est une fonction symétrique des racines de l'équation $f(x) = 0$; par conséquent, v_1 est exprimable rationnellement par les coefficients de f et de θ; et si ces quantités sont toutes réelles, v_1 ne contiendra d'autres imaginaires que celles de la racine α. En outre, $v_{\mu-1}$ se déduit de v_1 en remplaçant α par l'expression conjuguée $\alpha^{\mu-1}$; d'où il résulte que v_1 et $v_{\mu-1}$ sont des quantités connues imaginaires et conjuguées. On pourra donc poser

$$(9)\qquad \begin{cases} v_1 = \rho\left(\cos\omega + \sqrt{-1}\sin\omega\right), \\ v_{\mu-1} = \rho\left(\cos\omega - \sqrt{-1}\sin\omega\right). \end{cases}$$

Nous avons aussi, en général,

$$\left(\sqrt[\mu]{v_1}\right)^{\mu-n}\sqrt[\mu]{v_n} = a_n,$$

et, pour $n = \mu - 1$,

$$(10)\qquad \sqrt[\mu]{v_1}\,\sqrt[\mu]{v_{\mu-1}} = a_{\mu-1}.$$

$a_{\mu-1}$ est exprimable rationnellement par les coefficients de f et de θ, elle ne peut donc renfermer d'autres imaginaires que celle qui se trouve dans α. Mais il est évident

que $a_{\mu-1}$ ne change pas si l'on remplace α par $\alpha^{\mu-1}$ qui est sa conjuguée; donc $a_{\mu-1}$ est réelle.

Des équations (9) et (10) on déduit

$$\rho^2 = a_{\mu-1}^{\mu},$$

et, en désignant par a la valeur numérique de $a_{\mu-1}$,

$$\sqrt[\mu]{\rho} = \sqrt{a}.$$

La première des équations (9) donne alors cette valeur de $\sqrt[\mu]{v_1}$,

$$\sqrt[\mu]{v_1} = \sqrt{a}\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{\mu}\right),$$

où k désigne un nombre entier, et l'expression des racines x, donnée par l'équation (8), prend cette forme très-remarquable,

$$x = \frac{1}{\mu}\left\{\begin{aligned} &-A + \sqrt{a}\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{\mu}\right),\\ &+(f + g\sqrt{-1})\quad\left[\cos\frac{2(\omega + 2k\pi)}{\mu} + \sqrt{-1}\sin\frac{2(\omega + 2k\pi)}{\mu}\right]\\ &+(f_1 + g_1\sqrt{-1})\sqrt{a}\left[\cos\frac{3(\omega + 2k\pi)}{\mu} + \sqrt{-1}\sin\frac{3(\omega + 2k\pi)}{\mu}\right]\\ &+(f_2 + g_2\sqrt{-1})\quad\left[\cos\frac{4(\omega + 2k\pi)}{\mu} + \sqrt{-1}\sin\frac{4(\omega + 2k\pi)}{\mu}\right]\\ &+\ldots \end{aligned}\right\},$$

où a, f, g, f_1, g_1, etc., sont des fonctions rationnelles de $\cos\frac{2\pi}{\mu}$ et de $\sin\frac{2\pi}{\mu}$.

L'équation précédente fera connaître les μ racines de $f(x) = 0$, en donnant au nombre entier k les μ valeurs $0, 1, 2, 3, \ldots, \mu - 1$. De là résulte le théorème suivant :

Théorème. — *Pour résoudre l'équation* (1), $f(x) = 0$, *il suffit :*

1°. *De diviser la circonférence entière du cercle en* μ *parties égales; 2° de diviser ensuite un angle* ω *qu'on peut construire en* μ *parties égales; 3° d'extraire la racine carrée d'une seule quantité* a.

Remarque. — Les coefficients de f et de θ étant tous réels, si une racine de $f(x) = 0$ est réelle, toutes les autres le sont aussi; puisque, si x désigne cette racine réelle, les autres racines sont

$$\theta x,\quad \theta^2 x,\ldots,\quad \theta^{\mu-1} x.$$

Par conséquent, les racines de l'équation proposée sont toutes réelles, ou toutes imaginaires.

Première méthode particulière relative aux équations dont le degré est un nombre composé.

La méthode qui vient d'être exposée pour la résolution algébrique de l'équation

$$(1)\qquad f(x) = 0$$

est applicable à tous les cas, que μ soit premier ou non; mais, quand μ est un nombre composé, on peut simplifier la solution en opérant comme nous allons l'indiquer.

Soit $\mu = mn$. Les racines de l'équation (1) étant toujours

$$x,\quad \theta x,\quad \theta^2 x,\ldots,\quad \theta^{\mu-1} x,$$

nous pourrons les partager en m groupes de la manière suivante :

$$(2)\qquad \left\{\begin{array}{lllll} x, & \theta^{m} x; & \theta^{2m} x, & \ldots, & \theta^{(n-1)m} x, \\ \theta x, & \theta^{m+1} x, & \theta^{2m+1} x, & \ldots, & \theta^{(n-1)m+1} x, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \theta^{m-1} x, & \theta^{2m-1} x, & \theta^{3m-1} x, & \ldots, & \theta^{nm-1} x; \end{array}\right.$$

ou, en posant,

$$x = x_1, \quad \theta x = x_2, \quad \theta^2 x = x^3, \ldots, \quad \theta^{m-1} x = x_m,$$

et

$$\theta^m x = \theta_1 x,$$

de la manière suivante :

$$(2) \quad \left\{ \begin{array}{lllll} x_1, & \theta_1 x_1, & \theta_1^2 x_1, \ldots, & \theta_1^{n-1} x_1, \\ x_2, & \theta_1 x_2, & \theta_1^2 x_2, \ldots, & \theta_1^{n-1} x_2, \\ \ldots & & & \\ \ldots & & & \\ x_m, & \theta_1 x_m, & \theta_1^2 x_m, \ldots, & \theta_1^{n-1} x_m. \end{array} \right.$$

En appliquant donc à l'équation (1) la méthode exposée dans la leçon précédente, on pourra la décomposer en m équations, chacune du degré n, qui auront respectivement pour racines les racines des divers groupes (2), et dont les coefficients seront des fonctions rationnelles d'une même racine d'une équation

$$(3) \qquad \psi(y) = 0$$

de degré m. Soient

$$y_1, \quad y_2, \ldots, \quad y_m,$$

les m racines de l'équation (3), et

$$(4) \quad \varphi(x, y_1) = 0, \quad \varphi(x, y_2) = 0, \ldots, \quad \varphi(x, y_m) = 0,$$

les m équations qui ont respectivement pour racines les quantités du premier groupe (2), du deuxième, etc., du dernier. Je dis que, pour résoudre l'équation (1), il suffit de connaître une racine y de l'équation (3), et ensuite une racine x de l'équation

$$(5) \qquad \varphi(x, y) = 0$$

correspondante; car on aura, de cette manière, une racine (x) de l'équation (1), et les autres seront

$$\theta x, \quad \theta^2 x, \ldots, \quad \theta^{n-1} x.$$

L'équation proposée (1) étant résoluble algébriquement, l'équation (3) l'est aussi; car y désigne une fonction rationnelle de x. Mais je dis de plus que l'équation (3) jouit de la même propriété que l'équation (1), et que, par conséquent, on pourra lui appliquer la méthode de résolution précédemment exposée.

En effet, les racines de l'équation (1), renfermées dans le premier des groupes (2), sont

$$(6) \qquad x,\ \theta^m x,\ \theta^{2m} x, \ldots,\ \theta^{(n-1)m} x,$$

et y désigne une fonction rationnelle et symétrique de ces racines, c'est-à-dire une fonction rationnelle de x. Posons

$$y = \mathrm{F}(x,\ \theta^m x,\ \theta^{2m} x, \ldots,\ \theta^{(n-1)m} x) = \mathrm{F}(x),$$

les m racines $y_1, y_2, \ldots, y_m$ de l'équation (3) seront

$$\mathrm{F}(x),\ \mathrm{F}(\theta x),\ \mathrm{F}(\theta^2 x), \ldots,\ \mathrm{F}(\theta^{m-1} x),$$

et l'on aura

$$\mathrm{F}(\theta x) = \mathrm{F}(\theta x,\ \theta\theta^m x,\ \theta\theta^{2m} x, \ldots,\ \theta\theta^{(n-1)m} x).$$

Par conséquent, $\mathrm{F}(\theta x)$ et $\mathrm{F}(x)$ sont des fonctions rationnelles et symétriques des quantités (6), et l'on pourra exprimer rationnellement l'une par l'autre à l'aide de la méthode des fonctions semblables rappelée dans la dernière leçon.

Soit donc

$$\mathrm{F}(\theta x) = \lambda \mathrm{F}(x) = \lambda y,$$

λx étant une fonction rationnelle de x, on aura

$$\mathrm{F}(\theta^2 x) = \lambda \mathrm{F}(\theta x) = \lambda^2 y,$$
$$\mathrm{F}(\theta^3 x) = \lambda \mathrm{F}(\theta^2 x) = \lambda^3 y,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\mathrm{F}(\theta^{m-1} x) = \lambda \mathrm{F}(\theta^{m-2} x) = \lambda^{m-1} y,$$

et l'on voit que les m racines de l'équation (3) pourront être représentées par

$$y,\ \lambda y,\ \lambda^2 y,\ \ldots,\ \lambda^{m-1} y,$$

λ désignant une fonction rationnelle telle que $\lambda^m y = y$.

L'équation (3) une fois résolue, y sera connue, et l'on pourra appliquer à l'équation (5) la méthode précédemment exposée, puisque ses n racines peuvent être représentées par

$$x,\ \theta_1 x,\ \theta_1^2 x,\ldots,\ \theta_1^{n-1} x.$$

On peut donc énoncer le théorème suivant :

Si $\mu = mn$, la résolution de l'équation (1) *est ramenée à celle de deux équations des degrés m et n respectivement, et qui ont la même propriété que la proposée.*

Si n est lui-même un nombre composé $m_1 n_1$, on ramènera, de la même manière, la résolution de l'équation (5) à celle d'une équation en z

$$(7) \qquad \psi_1(z, y) = 0$$

de degré m_1, et à celle d'une équation en x de degré n_1

$$(8) \qquad \varphi_1(x, y, z) = 0.$$

Dans l'équation (7), y fait partie des quantités connues, et dans l'équation (8) il en est de même de y et de z. Et, généralement, on a ce théorème :

THÉORÈME. — *Si $\mu = m_1 m_2 \ldots m_n$, la résolution de l'équation* (1) *est ramenée à celle de n équations des degrés*

$$m_1,\ m_2,\ldots,\ m_n,$$

respectivement, et il suffit même de connaître une racine

de chacune de ces équations, qui ont toutes la même propriété que l'équation proposée.

Corollaire I. — *Si, en décomposant μ en facteurs premiers, on a*

$$\mu = \varepsilon_1^{p_1}\varepsilon_2^{p_2}\ldots\varepsilon_\omega^{p_\omega},$$

la résolution de l'équation proposée de degré μ se ramènera à celle de p_1 équations du degré ε_1, de p_2 équations du degré ε_2,..., de p_ω équations du degré ε_ω.

Corollaire II. — *Toute équation de degré 2^p, dont les racines peuvent être représentées par*

$$\theta x,\quad \theta^2 x,\ldots,\quad \theta^{2^p} x = x,$$

peut être résolue à l'aide de p extractions de racines carrées.

Exemple. — Supposons $\mu = 30$, les racines de

$$(1)\qquad f(x) = 0$$

seront

$$x,\ \theta x,\ \theta^2 x,\ldots,\ \theta^{29} x.$$

Comme $30 = 2\times 15$, on prendra pour y une fonction rationnelle et symétrique des quinze racines

$$x,\ \theta^2 x,\ \theta^4 x,\ldots,\ \theta^{28} x;$$

y dépendra d'une équation du second degré

$$(2)\qquad y^2 + \mathrm{A}y + \mathrm{B} = 0,$$

dont les coefficients seront immédiatement exprimables par ceux de la proposée; on pourrait former ensuite l'équation du quinzième degré ayant pour racines x, $\theta^2 x,\ldots,\theta^{28} x$, mais il est inutile de faire ce calcul : re-

présentons, comme précédemment, par

$$\varphi(x, y) = 0$$

cette équation, où y est une quantité connue. Comme $15 = 3 \times 5$, on prendra pour z une fonction rationnelle et symétrique des cinq racines

$$x,\ \theta^6 x,\ \theta^{12} x,\ \theta^{18} x,\ \theta^{24} x;$$

z dépendra d'une équation du troisième degré

$$(3) \qquad z^3 + Cz^2 + Dz + E = 0,$$

dont les coefficients seront des fonctions rationnelles de y et des autres quantités connues; enfin on formera l'équation

$$(4) \qquad x^5 + Fx^4 + Gx^3 + Hx^2 + Kx + L = 0,$$

qui a pour racines

$$x,\ \theta^6 x,\ \theta^{12} x,\ \theta^{18} x,\ \theta^{24} x,$$

et dont les coefficients seront des fonctions rationnelles de y et de z. La résolution de l'équation (1) sera ainsi ramenée à trouver une racine de l'équation (2), puis une racine de l'équation (3), puis enfin une racine de l'équation (4).

Deuxième méthode.

Revenons au cas général, et supposons

$$\mu = m_1 m_2 \ldots m_\omega.$$

Désignons par $n_1, n_2, \ldots, n_\omega$ les quotients respectifs de μ par $m_1, m_2, \ldots, m_\omega$, on aura

$$\mu = m_1 n_1 = m_2 n_2 = m_3 n_3 = \ldots = m_\omega n_\omega.$$

Cela posé, on peut, d'après ce qui précède, ramener la résolution de l'équation

$$f(x) = 0$$

à celle de deux équations, des ω manières suivantes :

(1) $\varphi_1(x, y_1) = 0$ ayant pour racines x, $\theta^{m_1}x$, $\theta^{2m_1}x, \ldots$, $\theta^{(n_1-1)m_1}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_1 d'une équation $\psi_1(y_1) = 0$ de degré m_1;

(2) $\varphi_2(x, y_2) = 0$ ayant pour racines x, $\theta^{m_2}x$, $\theta^{2m_2}x, \ldots$, $\theta^{(n_2-1)m_2}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_2 d'une équation $\psi_2(y_2) = 0$ de degré m_2;

....

....

(ω) $\varphi_\omega(x, y_\omega) = 0$ ayant pour racines x, $\theta^{m_\omega}x$, $\theta^{2m_\omega}x, \ldots$, $\theta^{(n_\omega-1)m_\omega}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_ω d'une équation $\psi_\omega(y_\omega) = 0$ de degré m^ω.

Supposons maintenant que $m_1, m_2, \ldots, m_\omega$ soient premiers entre eux, les équations

$$\varphi_1(x, y_1) = 0, \quad \varphi_2(x, y_2) = 0, \ldots, \quad \varphi_\omega(x, y_\omega) = 0$$

n'auront que la seule racine x commune; donc, d'après un théorème connu, on pourra exprimer x rationnellement par les coefficients de ces équations, et, par conséquent, en fonction rationnelle de $y_1, y_2, \ldots, y_\omega$. Ces dernières quantités étant connues, on aura une racine de l'équation (1), et, par suite, toutes les racines.

La résolution de l'équation (1) est donc ramenée à

trouver une racine de chacune des équations

$$\psi_1(y_1) = 0, \quad \psi_2(y_2) = 0, \ldots, \quad \psi_\omega(y_\omega) = 0,$$

qui sont respectivement des degrés $m_1, m_2, \ldots, m_\omega$. En outre, ces équations ont la même propriété que la proposée, ainsi que nous l'avons établi précédemment; on pourra donc leur appliquer la même méthode. Si l'on veut que ces équations soient les moins élevées possibles, et si, en décomposant μ en facteurs premiers, on a

$$\mu = \varepsilon_1^{p_1} \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega},$$

il faudra prendre

$$m_1 = \varepsilon_1^{p_1}, \quad m_2 = \varepsilon_2^{p_2}, \ldots, \quad m_\omega = \varepsilon_\omega^{p_\omega}.$$

Quant à la résolution de chacune des équations

$$\psi(y) = 0$$

de degré ε^p, elle se ramène à celle de p équations de degré ε, ainsi que nous l'avons démontré.

VINGT-HUITIÈME LEÇON.

Résolution algébrique des équations dont dépend la division de la circonférence du cercle en un nombre premier de parties égales. — Division de la circonférence en dix-sept parties égales. — Construction géométrique.

Résolution algébrique des équations dont dépend la division de la circonférence du cercle en un nombre premier de parties égales.

Le problème de la division du cercle en un nombre m quelconque de parties égales se ramène à la résolution de l'équation binôme

(1) $$z^m - 1 = 0;$$

car, si l'on fait

$$\frac{2\pi}{m} = a,$$

on obtiendra les m racines de l'équation précédente, en donnant à k les m valeurs

$$0,\quad 1,\quad 2,\quad 3,\ldots,\quad (m-1)$$

dans la formule

$$z = \cos ka + \sqrt{-1}\sin ka;$$

on connaîtra donc $\cos ka$ et $\sin ka$ lorsque l'équation binôme (1) sera résolue algébriquement.

Si m est un nombre impair $2\mu+1$, il vient, en divi-

sant l'équation (1) par $z-1$, et posant ensuite

$$z+\frac{1}{z}=x,$$

$$(2)\begin{cases} x^{\mu}+x^{\mu-1}-(\mu-1)x^{\mu-2}-(\mu-2)x^{\mu-3} \\ \quad +\frac{(\mu-2)(\mu-3)}{1.2}x^{\mu-4}+\frac{(\mu-3)(\mu-4)}{1.2}x^{\mu-5}-\ldots=0. \end{cases}$$

C'est de cette équation (2) que dépend directement la division du cercle en $2\mu+1$ parties égales. Ses μ racines sont représentées par la formule

$$x=2\cos\frac{2k\pi}{2\mu+1}=2\cos ka,$$

dans laquelle on doit donner à k les μ valeurs

$$1,\quad 2,\quad 3,\ldots,\quad \mu,$$

ou des valeurs qui ne diffèrent de celles-là que par des multiples de $2\mu+1$.

Nous avons vu, dans la treizième leçon, que si m ou $2\mu+1$ est un nombre composé, la résolution de l'équation (1) se ramène à la résolution d'autres équations de la même forme, et qui ont pour degrés respectifs les nombres premiers ou les puissances de nombres premiers qui divisent m. Dès lors, la même chose peut se dire de l'équation (2), et on peut se borner à considérer le cas où $m=2\mu+1$ est un nombre premier ou une puissance d'un nombre premier. Lorsque m est premier, nous ferons voir que la division de la circonférence en m parties égales exige seulement la résolution de plusieurs équations qui ont respectivement pour degrés les facteurs premiers égaux ou inégaux dans lesquels se décompose le nombre $m-1$. Au contraire, lorsque m est une puissance d'un nombre premier p, telle que p^i, la division de la circonférence en

m parties égales exige d'abord la division en p parties égales, et, en outre, la résolution de $i-1$ équations de degré p, qu'on ne peut éviter en aucune façon. Chacune de ces $i-1$ équations de degré p est résoluble algébriquement; cela résulte soit de la formule de Moivre, soit des considérations développées dans la treizième leçon.

Supposons donc $2\mu+1$ premier, et soit n une racine primitive pour ce nombre premier; je dis que les μ racines de l'équation (2) seront

$$(3)\qquad 2\cos a,\quad 2\cos na,\quad 2\cos n^2 a,\ldots,\quad 2\cos n^{\mu-1} a.$$

Il est évident que chacune de ces μ quantités satisfait à l'équation (2); il suffit donc de démontrer qu'elles sont toutes distinctes. Supposons, s'il est possible, que deux de ces quantités soient égales, et que l'on ait

$$2\cos n^p a = 2\cos n^q a,$$

p et q étant $<\mu$; on aurait

$$n^p a \pm n^q a = 2\lambda\pi,$$

λ désignant un nombre entier. Mais $a=\frac{2\pi}{2\mu+1}$, donc

$$\frac{n^q(n^{p-q}\pm 1)}{2\mu+1}$$

serait un nombre entier; et comme $2\mu+1$ est premier, que $n<2\mu+1$, il s'ensuit que $2\mu+1$ diviserait l'un des deux nombres $n^{p-q}+1$ ou $n^{p-q}-1$; il diviserait donc leur produit

$$n^{2p-2q}-1:$$

or ceci est impossible, car $2p-2q$ est $<2\mu$, et n désigne une racine primitive de $2\mu+1$. Donc les quantités (3) sont bien toutes les racines de l'équation (2).

Si maintenant on fait

$$x = 2\cos a, \quad \theta x = 2\cos na,$$

on aura

$$\theta^2 x = 2\cos n^2 a,\ \theta^3 x = 2\cos n^3 a, \ldots,\ \theta^{\mu-1} x = 2\cos n^{\mu-1} a,$$

et les racines de l'équation (2) seront représentées par

$$x,\quad \theta x,\quad \theta^2 x, \ldots,\quad \theta^{\mu-1} x;$$

on a, en outre, $\theta^\mu x = x$; car n étant une racine primitive de $2\mu+1$, on a $n^\mu \equiv -1$ (mod. $2\mu+1$); enfin θx est une fonction rationnelle de x, car $\cos na$ est exprimable rationnellement en fonction de $\cos a$. On voit donc que l'équation (2) est comprise dans la classe d'équations que nous avons étudiée dans la dernière leçon, et l'on pourra la résoudre par la méthode que nous avons exposée.

Ici, la fonction rationnelle θx a pour valeur (*voir* quatorzième leçon)

$$\theta x = x^n - n x^{n-2} + \frac{n(n-3)}{1.2} x^{n-4} - \frac{n(n-4)(n-5)}{1.2.3} x^{n-6} + \ldots.$$

En appliquant à l'équation (2) les théorèmes de la leçon précédente, on obtient les énoncés suivants :

1°. *Si $\mu = m_1 m_2 \ldots m_\omega$, on peut diviser la circonférence entière du cercle en $2\mu+1$ parties égales à l'aide de ω équations des degrés $m_1, m_2, \ldots, m_\omega$ respectivement. Si les nombres $m_1, m_2, \ldots, m_\omega$ sont premiers entre eux, les coefficients de ces équations seront des nombres rationnels.*

2°. *Si $\mu = 2^\omega$, on pourra diviser la circonférence du*

cercle en $2\mu+1$ *parties égales, à l'aide de* ω *racines carrées. En d'autres termes, si* $2\mu+1$ *est un nombre premier, et* $\mu = 2^{\omega}$, *on pourra diviser la circonférence du cercle en* $2\mu+1$ *parties égales, avec la règle et le compas.*

3°. *Pour diviser la circonférence du cercle en* $2\mu+1$ *parties égales, il suffit de diviser la circonférence entière en* 2μ *parties égales, de diviser un arc, qu'on peut construire ensuite en* 2μ *parties égales, et d'extraire la racine carrée d'une seule quantité.*

Ce dernier théorème est dû à M. Gauss. Ce géomètre a prouvé, en outre, que la quantité dont il faut extraire la racine carrée est simplement le nombre entier $2\mu+1$. Voici comment Abel le démontre.

En désignant par ρ cette quantité, ρ est, comme nous l'avons vu dans la leçon précédente, la valeur numérique du produit

$$(x+\alpha\theta x+\alpha^2\theta^2 x+\ldots+\alpha^{\mu-1}\theta^{\mu-1}x)(x+\alpha^{\mu-1}\theta x+\alpha^{\mu-2}\theta^2 x+\ldots+\alpha\theta^{\mu-1}x),$$

où

$$\alpha = \cos\frac{2\pi}{\mu} + \sqrt{-1}\sin\frac{2\pi}{\mu}.$$

On a donc

$$\pm\rho = 4(\cos a + \alpha\cos na + \alpha^2\cos n^2 a + \ldots + \alpha^{\mu-1}\cos n^{\mu-1}a)$$
$$\times(\cos a + \alpha^{\mu-1}\cos na + \alpha^{\mu-2}\cos n^2 a + \ldots + \alpha\cos n^{\mu-1}a).$$

En développant ce produit, on aura un résultat de la forme

$$\pm\rho = t_0 + t_1\alpha + t_2\alpha^2 + \ldots + t_{\mu-1}\alpha^{\mu-1},$$

et l'on trouve facilement

$$= 4(\cos a\cos n^m a + \cos na\cos n^{m+1}a + \ldots + \cos n^{\mu-1-m}a\cos n^{\mu-1}a)$$
$$+ 4(\cos n^{\mu-m}a\cos a + \cos n^{\mu-m+1}a\cos na + \ldots + \cos n^{\mu-1}a\cos n^{m-1}a).$$

En se servant de la formule

$$\cos n^p a \cos n^{m+p} a = \frac{1}{2}\cos(n^{m+p} a + n^p a) + \frac{1}{2}\cos(n^{m+p} a - n^p a),$$

la valeur de t_m prendra la forme

$$t_m = 2\left[\begin{array}{c}\cos(n^m+1)a + \cos(n^m+1)na + \cos(n^m+1)n^2a + \ldots \\ + \cos(n^m+1)n^{\mu-1}a\end{array}\right]$$
$$+ 2\left[\begin{array}{c}\cos(n^m-1)a + \cos(n^m-1)na + \cos(n^m-1)n^2a + \ldots \\ + \cos(n^m-1)n^{\mu-1}a\end{array}\right],$$

ou, en faisant

$$(n^m+1)a = a', \quad (n^m-1)a = a'',$$

$$t_m = 2\cos a' + \theta\, 2\cos a' + \theta^2\, 2\cos a' + \ldots + \theta^{\mu-1}\, 2\cos a'$$
$$+ 2\cos a'' + \theta\, 2\cos a'' + \theta^2\, 2\cos a'' + \ldots + \theta^{\mu-1}\, 2\cos a''.$$

Cela posé, supposons d'abord que m ne soit pas nul; $2\cos a'$ et $2\cos a''$ sont des racines de l'équation (2), donc

$$2\cos a' = \theta^{\delta} x \quad \text{et} \quad 2\cos a'' = \theta^{\varepsilon} x,$$

et l'on aura

$$t_m = \left(\theta^{\delta} x + \theta^{\delta+1} x + \ldots + \theta^{\mu-1} x + x + \theta x \ldots + \theta^{\delta-1} x\right)$$
$$+ \left(\theta^{\varepsilon} x + \theta^{\varepsilon+1} x + \ldots + \theta^{\mu-1} x + \theta x + \ldots\ldots + \theta^{\varepsilon-1} x\right),$$

ou

$$t_m = 2\left(x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x\right);$$

c'est-à-dire que t_m est double de la somme des racines de l'équation (2), laquelle est égale à -1; on a donc

$$t_m = -2.$$

Supposons maintenant $m = 0$, on aura

$$t_0 = 2\left(\cos 2a + \cos 2na + \cos 2n^2a + \ldots + \cos 2n^{\mu-1}a\right) + 2\mu.$$

Or $2\cos 2a$ est racine de l'équation (2); donc, en faisant

$$2\cos 2a = \theta^{\delta} x,$$

on aura

$$t_0 = \left(\theta^{\delta} x + \theta^{\delta+1} x + \ldots + \theta^{\mu-1} x + x + \theta x + \ldots + \theta^{\delta-1} x\right) + 2\mu,$$

et, par conséquent,

$$t_0 = 2\mu - 1.$$

D'après cela, la valeur de $\pm\rho$ sera

$$\pm\rho = 2\mu - 1 - 2\left(\alpha + \alpha^2 + \ldots + \alpha^{\mu-1}\right).$$

D'ailleurs

$$\alpha + \alpha^2 + \ldots + \alpha^{\mu-1} = -1,$$

donc

$$\pm\rho = 2\mu + 1.$$

Ce qu'il fallait démontrer.

La théorie que nous venons d'exposer conduit à un grand nombre de conséquences importantes. On en verra un exemple remarquable dans la Note X.

Division de la circonférence en dix-sept parties égales.

En faisant $2\mu + 1 = 17$ ou $\mu = 8$, l'équation (2) du paragraphe précédent devient

$$(1)\quad x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 - 10x^3 - 10x^2 - 4x + 1 = 0,$$

et ses racines, comprises dans la formule

$$x = 2\cos\frac{2k\pi}{17},$$

peuvent être représentées par

(2) $x,\ \theta x,\ \theta^2 x,\ \theta^3 x,\ \theta^4 x,\ \theta^5 x,\ \theta^6 x,\ \theta^7 x.$

La plus petite racine primitive de 17 est 3 (*voir* la Table des racines primitives, page 340), et les résidus par rapport à 17 des puissances

$$3^0,\ 3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6,\ 3^7,$$

sont

$$1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11;$$

donc, en faisant, pour abréger,

$$a = \frac{2\pi}{17},$$

les quantités (2) seront

$$2\cos a,\quad 2\cos 3a,\quad 2\cos 9a,\quad 2\cos 10a,$$
$$2\cos 13a,\quad 2\cos 5a,\quad 2\cos 15a,\quad 2\cos 11a;$$

ou, à cause de $\cos(17 - m)a = \cos a$,

$$2\cos a,\quad 2\cos 3a,\quad 2\cos 8a,\quad 2\cos 7a,$$
$$2\cos 4a,\quad 2\cos 5a,\quad 2\cos 2a,\quad 2\cos 6a.$$

Pour appliquer la méthode générale, il faut commencer par calculer une fonction rationnelle et symétrique y des quantités

$$2\cos a,\quad 2\cos 8a,\quad 2\cos 4a,\quad 2\cos 2a.$$

Posons donc

$$y = 2\cos a + 2\cos 8a + 2\cos 4a + 2\cos 2a;$$

y dépendra d'une équation du second degré, dont les deux racines seront

(3) $y = 2\cos a + 2\cos 8a + 2\cos 4a + 2\cos 2a,$

(4) $y_1 = 2\cos 3a + 2\cos 7a + 2\cos 5a + 2\cos 6a.$

Cette équation est bien aisée à former, car on a d'abord,

par l'équation (1),

$$(5) \qquad y + y_1 = -1;$$

ensuite, en multipliant y par y_1, transformant les produits de cosinus en sommes à l'aide des formules connues, et ayant égard à l'équation identique

$$\cos(17 - m)a = \cos ma,$$

on trouve

$$yy_1 = 4\begin{pmatrix} 2\cos a + 2\cos 2a + 2\cos 3a + 2\cos 4a + 2\cos 5a \\ + 2\cos 6a + 2\cos 7a + 2\cos 8a \end{pmatrix},$$

et, à cause de l'équation (1),

$$(6) \qquad yy_1 = -4.$$

L'équation en y sera donc

$$(7) \qquad y^2 + y - 4 = 0,$$

et l'on peut considérer comme connues ses deux racines y et y_1.

Maintenant les quantités

$$2\cos a, \quad 2\cos 8a, \quad 2\cos 4a, \quad 2\cos 2a,$$

sont racines d'une équation du quatrième degré dont les coefficients sont fonctions rationnelles de y, et sur laquelle nous allons raisonner comme nous avons fait sur la proposée. Il faut, conformément à la méthode générale, chercher d'abord une fonction rationnelle et symétrique z des quantités

$$2\cos a, \quad 2\cos 4a.$$

Posons donc

$$z = 2\cos a + 2\cos 4a,$$

l'équation en z sera du second degré, et aura pour racines

$$(8) \qquad z = 2\cos a + 2\cos 4a,$$

$$(9) \qquad z_1 = 2\cos 8a + 2\cos 2a.$$

On a d'abord

(10) $$z + z_1 = y,$$

et en multipliant z par z_1, on trouve, après avoir remplacé les produits de cosinus par des sommes,

$$zz_1 = \begin{pmatrix} 2\cos a + 2\cos 2a + 2\cos 3a + 2\cos 4a + 2\cos 5a \\ + 2\cos 6a + 2\cos 7a + 2\cos 8a \end{pmatrix},$$

ou, à cause que la somme des racines de l'équation (1) est -1,

(11) $$zz_1 = -1;$$

l'équation en z sera donc

(12) $$z^2 - yz - 1 = 0.$$

Enfin il ne reste plus qu'à former l'équation du second degré dont les racines sont

$$2\cos a, \quad 2\cos 4a,$$

et dont les coefficients peuvent s'exprimer en fonction rationnelle de y et de z. Mais on peut simplifier ici l'application de la méthode générale.

Considérons l'équation du quatrième degré, dont les racines

$$2\cos 3a, \quad 2\cos 7a, \quad 2\cos 5a, \quad 2\cos 6a$$

ont pour somme y_1, et opérons comme nous avons fait à l'égard de l'équation qui a pour racines les quantités dont la somme est y. On formera une équation du second degré ayant pour racines

(13) $$u = 2\cos 3a + 2\cos 5a,$$

(14) $$u_1 = 2\cos 7a + 2\cos 6a,$$

et, en opérant comme précédemment, on trouvera

(15) $$u + u_1 = y_1,$$

(16) $$uu_1 = -1;$$

cette équation en u sera donc

$$(17) \qquad u^2 - y_1 u - 1 = 0,$$

et les quantités u et u_1 sont connues ainsi que z et z_1.

Cela posé, faisons

$$(18) \qquad x = 2\cos a,$$

$$(19) \qquad x_1 = 2\cos 4a;$$

on aura d'abord

$$(20) \qquad x + x_1 = z,$$

et ensuite

$$xx_1 = 4\cos a\cos 4a = 2\cos 3a + 2\cos 5a$$

ou

$$(21) \qquad xx_1 = u;$$

x et x_1 seront donc racines de l'équation

$$(22) \qquad x^2 - zx + u = 0.$$

La résolution de l'équation (1) est ainsi ramenée à celle des équations du second degré (7), (12), (17) et (22); le problème est donc résolu. Nous allons chercher maintenant à déduire de l'analyse précédente une construction géométrique, pour effectuer la division de la circonférence en dix-sept parties égales.

Construction géométrique.

Quand on se propose, dans la géométrie élémentaire, d'inscrire dans un cercle les polygones réguliers de trois et de cinq côtés, on commence par inscrire ceux de six et de dix côtés. De même, nous commencerons ici par

inscrire le polygone régulier de trente-quatre côtés, celui de dix-sept côtés s'en déduira immédiatement.

Soit une demi-circonférence (*fig.* 3), partagée en dix-sept parties égales aux points

$$a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ i,\ j,\ k,\ l,\ m,\ n,\ o,\ p,\ q,\ r;$$

la corde *ab* sera le côté du polygone régulier inscrit de trente-quatre côtés, et les cordes *ad*, *af*, *ah*, *aj*, *al*, *an*, *ap* seront les diagonales de ce polygone ou, si l'on veut, les côtés des polygones réguliers *étoilés* de trente-quatre côtés, que l'on peut inscrire dans la circonférence.

En prenant le rayon pour unité et faisant, comme précédemment,

$$a = \frac{2\pi}{17},$$

on aura

$$ab = 2 \sin \frac{\pi}{34} = +\ 2 \cos 4a,$$

$$ad = 2 \sin \frac{3\pi}{34} = -\ 2 \cos 5a,$$

$$af = 2 \sin \frac{5\pi}{34} = +\ 2 \cos 3a,$$

$$ah = 2 \sin \frac{7\pi}{34} = -\ 2 \cos 6a,$$

$$aj = 2 \sin \frac{9\pi}{34} = +\ 2 \cos 2a,$$

$$al = 2 \sin \frac{11\pi}{34} = -\ 2 \cos 7a,$$

$$an = 2 \sin \frac{13\pi}{34} = +\ 2 \cos a,$$

$$ap = 2 \sin \frac{15\pi}{34} = -\ 2 \cos 8a.$$

Conservons toutes les notations du paragraphe précédent;

les équations (3) et (4) nous donnent

$$y = an - ap + ab + aj,$$
$$y_1 = af - al - ad - ah.$$

On voit que y_1 est négatif, car af est $< al$; par suite, y est positif, puisque $yy_1 = -1$. Faisant donc $y_1 = -y'$, les équations (5) et (6) deviennent

$$y' - y = 1,$$
$$yy' = 4.$$

Les équations (8) et (9) nous donnent

$$z = an + ab,$$
$$z_1 = - ap + aj;$$

z_1 est négatif, car ap est $> aj$, et z est positif. Les équations (10) et (11) deviennent, en faisant $z_1 = - z'$,

$$z - z' = y,$$
$$zz' = 1.$$

Pareillement, les équations (13) et (14) donnent

$$u = af - ad,$$
$$u_1 = - al - ah;$$

u_1 est donc négatif, et u positif. Faisant $u_1 = - u'$, on aura, par les équations (15) et (16),

$$u' - u = y',$$
$$uu' = 1;$$

enfin les équations (18) et (19) donnent

$$x = an,$$
$$x_1 = ab,$$

en sorte que x et x_1 sont positifs, et les équations (20)

et (21) conservent leur forme

$$x + x_1 = z,$$
$$xx_1 = u.$$

Le côté de notre polygone de trente-quatre côtés est x_1, et, pour le construire, on voit qu'il suffit,

1°. De construire deux lignes y et y' telles, que

$$y' - y = 1, \quad yy' = 4;$$

2°. De construire quatre lignes z, z', u, u' telles, que

$$z - z' = y, \quad zz' = 1,$$
$$u' - u = y', \quad uu' = 1;$$

3°. De construire deux lignes x et x_1 telles, que

$$x + x_1 = z, \quad xx_1 = n.$$

Construction. 1°. En un point O d'une ligne indéfinie UV (*fig.* 4), élevons une perpendiculaire OA égale au rayon du cercle, c'est-à-dire à l'unité. Prenons $OC = \frac{1}{4}$, puis, du point C comme centre, avec CA pour rayon, décrivons un cercle qui coupe en B et D la ligne UV; on aura

$$OB = \frac{1}{2} y, \quad OD = \frac{1}{2} y';$$

car

$$2OD - 2OB = 4OC = 1 \quad \text{et} \quad 2OD \times 2OB = 4\overline{OA}^2 = 4.$$

2°. Joignons AB, et du point B comme centre, avec OB pour rayon, décrivons une circonférence qui coupe en M et P la ligne AB prolongée, on aura

$$OM = z, \quad AP = z';$$

car

$$AM - AP = PM = 2OB = y \quad \text{et} \quad AM.AP = \overline{AO}^2 = 1.$$

Joignons pareillement AD, et du point D comme centre, avec OD pour rayon, décrivons une circonférence qui coupe en N et Q la ligne AD prolongée, on aura

$$AN = u, \quad AQ = u';$$

car

$$AQ - AN = NQ = 2\,OD = y' \quad \text{et} \quad AN.AQ = \overline{AO}^2 = 1.$$

3°. Rabattons AO en AE sur le prolongement de AD, décrivons sur NE, comme diamètre, un cercle qui coupe AB en F; du point F comme centre, avec $AI = \frac{AM}{2}$ pour rayon, décrivons un cercle qui coupe AD en G; et, enfin, du point G comme centre, avec ce même rayon, décrivons un cercle qui coupe AD en K et H, on aura

$$x_1 = AK, \quad x = AH;$$

car

$$AK + AH = 2\,GF = 2\,AI = AM = z$$

et

$$AK.AH = \overline{AF}^2 = AN.AE = AN.AO = u.$$

Le côté du polygone régulier de trente-quatre côtés inscrit dans le cercle dont le rayon est OA, est donc égal à AK.

VINGT-NEUVIÈME LEÇON.

Formule de Lagrange pour le développement de certaines fonctions implicites. — Développement d'une racine de l'équation $z = x + tz^m$. — Autre application de la formule de Lagrange.

Formule de Lagrange pour le développement de certaines fonctions implicites.

Lagrange a donné, dans les *Mémoires de l'Académie de Berlin* pour l'année 1768, une formule remarquable, par laquelle on peut développer en série une classe étendue de fonctions implicites (*). Laplace a donné ensuite de cette même formule une démonstration très-simple, fondée sur le calcul intégral, et que Lagrange a introduite dans sa *Théorie des fonctions analytiques* (**). Plus tard, M. Cauchy en a publié une nouvelle, qui a l'avantage de faire connaître le reste de la série (***). Nous présenterons ici la démonstration très-simple et très-directe que M. Duhamel a donnée dans son *Cours de Mécanique de l'École Polytechnique* (****).

Soit une fonction z de deux variables indépendantes x

(*) *Voir* le *Traité de la Résolution des Équations numériques*, Note XI. Lagrange deduit sa formule de celle que nous faisons connaître dans la Note I.

(**) *Voir* la 3e édit. de cet ouvrage, que j'ai publiée en 1847, page 147.

(***) *Mémoires de l'Académie impériale des Sciences de l'Institut de France*, tome VIII, page 130.

(****) Deuxième partie, page 57.

et t, qui satisfait à l'équation

$$(1) \qquad z = x + tf(z),$$

où f désigne une fonction donnée quelconque. L'équation (1) admet généralement plusieurs racines z, mais nous achèverons de déterminer la fonction z que nous considérons, par la condition qu'elle se réduise à x pour $t = 0$. Cela posé, nous nous proposons de former le développement de z en série ordonnée suivant les puissances de t.

On a, par la formule de Maclaurin, en considérant z comme fonction de la seule variable t,

$$(2) \quad z = z_0 + \left(\frac{dz}{dt}\right)_0 t + \left(\frac{d^2 z}{dt}\right)_0 \frac{t^2}{1.2} + \ldots + \left(\frac{d^n z}{dt^n}\right)_0 \frac{t^n}{1.2\ldots n} + R_n,$$

z_0, $\left(\frac{dz}{dt}\right)_0, \ldots, \left(\frac{d^n z}{dt^n}\right)_0$ étant des valeurs de z et de ses dérivées pour $t = 0$, et R_n désignant le reste de la série.

En faisant $t = 0$ dans l'équation (1), on a d'abord

$$z_0 = x;$$

et il ne reste plus qu'à trouver généralement la valeur de $\frac{d^m z}{dt^m}$ pour $t = 0$.

Différentiant successivement l'équation (1) par rapport à chacune des variables x et t, on a

$$\frac{dz}{dx} = 1 + tf'(z)\frac{dz}{dx}, \quad \frac{dz}{dt} = f(z) + tf'(z)\frac{dz}{dt},$$

et, en éliminant $f'(z)$,

$$(3) \qquad \frac{dz}{dt} = f(z)\frac{dz}{dx}.$$

Cette équation fait connaître la valeur de $\left(\frac{dz}{dt}\right)_0$, car

pour $t=0$, on a

$$z = z_0 = x \quad \text{et} \quad \frac{dz}{dx} = 1;$$

donc

$$\left(\frac{dz}{dt}\right)_0 = f(x).$$

Pour avoir la valeur de $\left(\frac{d^2 z}{dt^2}\right)_0$, différentions l'équation (3) par rapport à t, et ensuite par rapport à x; on aura

$$\frac{d^2 z}{dt^2} = f(z)\frac{d^2 z}{dx\,dt} + f'(z)\frac{dz}{dx}\frac{dz}{dt},$$

$$\frac{d^2 z}{dx\,dt} = f(z)\frac{d^2 z}{dx^2} + f'(z)\left(\frac{dz}{dx}\right)^2;$$

en éliminant $\frac{d^2 z}{dx\,dt}$ entre ces équations, et remplaçant $\frac{dz}{dt}$ par sa valeur tirée de (3), il vient

$$\frac{d^2 z}{dt^2} = f(z)^2\frac{d^2 z}{dx^2} + 2f(z)f'(z)\left(\frac{dz}{dx}\right)^2,$$

et, comme le second membre est la dérivée de $f(z)^2\frac{dz}{dx}$ par rapport à x, on aura enfin

$$(4) \qquad \frac{d^2 z}{dt^2} = \frac{d\left[f(z)^2\frac{dz}{dx}\right]}{dx}.$$

Faisant maintenant

$$t=0, \quad z=x, \quad \frac{dz}{dx}=1,$$

il vient

$$\left(\frac{d^2 z}{dt^2}\right)_0 = \frac{df(x)^2}{dx}.$$

On peut continuer de la même manière pour former les

dérivées successives $\left(\frac{d^2z}{dt^2}\right)_0$, etc.; mais, pour éviter de répéter sans cesse les mêmes réductions, nous commencerons par établir une formule générale qui simplifiera l'exposition de la méthode.

Soit $\varphi(z)$ une fonction quelconque, et différentions

$$\varphi(z)\frac{dz}{dx}$$

par rapport à t, on aura

$$\frac{d\left[\varphi(z)\frac{dz}{dx}\right]}{dt}=\varphi'(z)\frac{dz}{dt}\frac{dz}{dx}+\varphi(z)\frac{d^2z}{dx\,dt},$$

ou, en mettant à la place de $\frac{dz}{dt}$ et de $\frac{d^2z}{dx\,dt}$ leurs valeurs précédemment écrites,

$$\frac{d\left[\varphi(z)\frac{dz}{dx}\right]}{dt}=[\varphi'(z)f(z)+\varphi(z)f'(z)]\left(\frac{dz}{dx}\right)^2+\varphi(z)f(z)\frac{d^2z}{dx^2}.$$

Le second membre est la dérivée de

$$\varphi(z)f(z)\frac{dz}{dx}$$

par rapport à x; on aura donc généralement

$$(5)\qquad \frac{d\left[\varphi(z)\frac{dz}{dx}\right]}{dt}=\frac{d\left[\varphi(z)f(z)\frac{dz}{dx}\right]}{dx}.$$

Au moyen de cette formule, on pourrait déduire l'équation (4) de (3), en supposant $\varphi(z)=f(z)$.

Faisons maintenant $\varphi(z)=f(z)^2$, l'équation (5) don-

nera

$$\frac{d\left[f(z)^2\frac{dz}{dx}\right]}{dt}=\frac{d\left[f(z)^3\frac{dz}{dx}\right]}{dx},$$

et, par conséquent, en différentiant l'équation (4) par rapport à t, on aura

$$\frac{d^3z}{dt^3}=\frac{d^2\left[f(z)^3\frac{dz}{dx}\right]}{dx^2};$$

en différentiant cette dernière par rapport à t, et se servant de l'équation (5) où l'on fera $\varphi(z)=f(z)^3$, on aura

$$\frac{d^4z}{dt^4}=\frac{d^3\left[f(z)^4\frac{dz}{dx}\right]}{dx^3};$$

et je dis que l'on a généralement

$$(6)\qquad \frac{d^mz}{dt^m}=\frac{d^{m-1}\left[f(z)^m\frac{dz}{dx}\right]}{dx^{m-1}}.$$

Comme nous avons établi cette formule pour les valeurs 1, 2, 3 de m, il suffit de démontrer que si elle a lieu pour une valeur quelconque de m, elle a lieu aussi pour cette même valeur de m augmentée d'une unité. Supposons donc que l'équation (6) ait lieu, et faisons $\varphi(z)=f(z)^m$ dans l'équation (5), on aura

$$\frac{d\left[f(z)^m\frac{dz}{dx}\right]}{dt}=\frac{d\left[f(z)^{m+1}\frac{dz}{dx}\right]}{dx};$$

différentions maintenant l'équation (6) par rapport à t,

il vient

$$\frac{d^{m+1}z}{dt^{m+1}} = \frac{d^m\left[f(z)^{m+1}\frac{dz}{dx}\right]}{dx^m},$$

équation qui se déduit de (6) en changeant m en $m+1$. L'équation (6) est donc générale, et, en y faisant $t=0$, il vient

$$\left(\frac{d^m z}{dt^m}\right)_0 = \frac{d^{m-1}f(x)^m}{dx^{m-1}}.$$

Le développement (2) de z sera donc

$$(7)\quad z = x + tf(x) + \frac{t^2}{1.2}\frac{df(x)^2}{dx} + \ldots + \frac{t^n}{1.2\ldots n}\frac{d^{n-1}f(x)^n}{dx^{n-1}} + R_n.$$

Proposons-nous maintenant de former le développement d'une fonction quelconque $F(z)$ de z en série ordonnée suivant les puissances croissantes de t.

On a, par la formule de Maclaurin,

$$(8)\quad \begin{cases} F(z) = F_0 + \left(\dfrac{dF}{dt}\right)_0 t + \left(\dfrac{d^2F}{dt^2}\right)_0 \dfrac{t^2}{1.2} + \ldots \\ \qquad + \left(\dfrac{d^nF}{dt^n}\right)_0 \dfrac{t^n}{1.2\,3\ldots} + R_n, \end{cases}$$

en désignant par F_0, $\left(\frac{dF}{dt}\right)_0$, etc., les valeurs de F et de ses dérivées pour $t=0$, et par R_n le reste de la série. Le premier terme F_0 est égal à $F(x)$, car on a $z=x$ pour $t=0$; il reste donc à déterminer généralement $\left(\frac{d^mF}{dt^m}\right)_0$.

On a d'abord

$$\frac{dF}{dt} = F'(z)\frac{dz}{dt} = F'(z)f(z)\frac{dz}{dx},$$

et, en différentiant par rapport à t,

$$\frac{d^2 F}{dt^2} = \frac{d\left[F'(z) f(z) \frac{dz}{dx}\right]}{dt};$$

mais l'équation (5) donne, en faisant $\varphi(z) = F'(z) f(z)$,

$$\frac{d\left[F'(z) f(z) \frac{dz}{dx}\right]}{dt} = \frac{d\left[F'(z) f(z)^2 \frac{dz}{dx}\right]}{dx},$$

donc

$$\frac{d^2 F}{dt^2} = \frac{d\left[F'(z) f(z)^2 \frac{dz}{dx}\right]}{dx}.$$

On déduira pareillement de cette dernière, en faisant usage de l'équation (5),

$$\frac{d^3 F}{dt^3} = \frac{d^2\left[F'(z) f(z)^3 \frac{dz}{dx}\right]}{dx^2},$$

et l'on ferait voir, comme précédemment, qu'on a généralement

(9) $$\frac{d^m F}{dt^m} = \frac{d^{m-1}\left[F'(z) f(z)^m \frac{dz}{dx}\right]}{dx^{m-1}};$$

faisant $t = 0$, $z = x$, $\frac{dz}{dx} = 1$, cette formule donne

$$\left(\frac{d^m F}{dt^m}\right)_0 = \frac{d^{m-1}[F'(x) f(x)^m]}{dx^{m-1}}.$$

Le développement (8) de $F(z)$ sera, par conséquent,

(10) $$\begin{cases} F(z) = F(x) + t F'(x) f(x) + \frac{t^2}{1.2} \frac{d[F'(x) f(x)^2]}{dx} + \ldots \\ \qquad + \frac{t^n}{1.2.3\ldots n} \frac{d^{n-1}[F'(x) f(x)^n]}{dx^{n-1}} + R_n. \end{cases}$$

Quant à la forme du reste, je ne crois pas devoir en parler ici, et je renverrai le lecteur au Mémoire dans lequel M. Cauchy a traité cette question.

Développement d'une racine de l'équation $z = x + tz^m$.

En faisant $f(z) = z^m$ dans l'équation (7), on a le développement suivant :

$$z = x + x^m t + \frac{2m}{1.2} x^{2m-1} t^2 + \frac{3m(3m-1)}{1.2.3} x^{3m-2} t^3 + \ldots$$
$$+ \frac{nm(nm-1)\ldots(nm-n+2)}{1.2.3\ldots n} x^{nm-n+1} t^n + \ldots,$$

pour celle des racines de l'équation

$$z = x + tz^m,$$

qui se réduit à x pour $t = 0$.

Le terme général u_n de cette série a pour valeur

$$u_n = \frac{nm(nm-1)\ldots(nm-n+2)}{1.2.3\ldots n} x^{nm-n+1} t^n;$$

et l'on en déduit

$$\frac{u_{n+1}}{u_n} = \frac{1}{n+1} \frac{(nm+m)(nm+m-1)\ldots(nm+1)}{(nm-n+2)\ldots(nm-n+m)} x^{m-1} t:$$

la limite de ce rapport, pour $n = \infty$, est égale à

$$\frac{m^m}{(m-1)^{m-1}} x^{m-1} t.$$

Il en résulte que la série précédente sera convergente, si cette quantité est inférieure à l'unité.

Autre application de la formule de Lagrange.

La formule de Lagrange est souvent utile pour le développement des fonctions explicites. Nous allons en donner un exemple. Supposons qu'on veuille développer la fonction $\frac{(\zeta-t)^m}{(1-t)^{m+1}}$ suivant les puissances croissantes de t.

En appliquant la formule de Lagrange à l'équation

$$z=\zeta+tf(z), \tag{1}$$

où z désigne une fonction des variables ζ et t, et $f(z)$ une fonction quelconque de z, il vient

$$F(z)=\sum\frac{t^n}{1.2\ldots n}\frac{d^{n-1}[F'(\zeta)f(\zeta)^n]}{d\zeta^{n-1}},$$

et, en différentiant par rapport à ζ,

$$F'(z)\frac{dz}{d\zeta}=\sum\frac{t^n}{1.2\ldots n}\frac{d^n[F'(\zeta)f(\zeta)^n]}{d\zeta^n}. \tag{2}$$

Maintenant soient

$$F'(z)=z^m \quad \text{et} \quad f(z)=z-1,$$

l'équation (1) donnera

$$z=\frac{\zeta-t}{1-t}, \quad \frac{dz}{d\zeta}=\frac{1}{1-t},$$

et, par suite, l'équation (2) devient

$$\frac{(\zeta-t)^m}{(1-t)^{m+1}}=\sum\frac{t^n}{1.2\ldots n}\frac{d^n\zeta^m(\zeta-1)^n}{d\zeta^n}.$$

TRENTIÈME LEÇON.

Solution d'un problème d'analyse indéterminé relatif à la représentation géométrique des fonctions elliptiques.

La question que je vais développer dans cette leçon est extraite du Mémoire *sur la représentation géométrique des fonctions elliptiques et ultrà-elliptiques*, que j'ai publié dans les tomes X et XI du Journal de M. Liouville, et qui fait partie du tome XI du *Recueil des Savants étrangers*.

Solution d'un problème d'analyse indéterminée relatif à la représentation géométrique des fonctions elliptiques.

Le problème que nous nous proposons de résoudre est le suivant :

Trouver toutes les solutions que peut admettre l'équation indéterminée

$$(1) \qquad dx^2 + dy^2 = \frac{c^2\,dz^2}{(z^2 - a^2)(z^2 - \alpha^2)},$$

où c est une constante réelle, a^2 et α^2 deux constantes imaginaires conjuguées, en ne prenant pour x et y que des fonctions réelles et rationnelles de z qui ne puissent être infinies que pour $z = \pm a$ et $z = \pm \alpha$.

Désignons, pour abréger, par i l'imaginaire $\sqrt{-1}$.

L'équation (1) peut s'écrire de la manière suivante :

$$(2)\qquad \frac{dx + i\,dy}{\left(\dfrac{c\,dz}{z^2 - a^2}\right)} \cdot \frac{dx - i\,dy}{\left(\dfrac{c\,dz}{z^2 - \alpha^2}\right)} = 1;$$

et comme x et y sont des fonctions réelles et rationnelles de z, les deux facteurs du premier membre de l'équation (2) sont des fonctions rationnelles imaginaires et conjuguées, ayant pour module l'unité. Donc, en désignant par p et ϖ deux polynômes imaginaires et conjugués, par ω un angle réel et par e la base des logarithmes népériens, on pourra poser

$$\frac{dx + i\,dy}{\left(\dfrac{c\,dz}{z^2 - a^2}\right)} = e^{\omega i}\frac{p}{\varpi}, \qquad \frac{dx - i\,dy}{\left(\dfrac{c\,dz}{z^2 - \alpha^2}\right)} = e^{-\omega i}\frac{\varpi}{p},$$

ou

$$(3)\qquad \begin{cases} dx + i\,dy = ce^{\omega i}\dfrac{p\,dz}{\varpi(z^2 - a^2)}, \\[2mm] dx - i\,dy = ce^{-\omega i}\dfrac{\varpi\,dz}{p(z^2 - \alpha^2)}. \end{cases}$$

La seconde de ces équations (3) se déduisant de la première par le changement de i en $-i$, il est inutile de la considérer; en intégrant la première, on a

$$(4)\qquad x + iy = ce^{\omega i}\int \frac{p}{\varpi}\,\frac{dz}{z^2 - a^2},$$

et il ne reste plus qu'à déterminer les polynômes p et ϖ, de manière que l'intégrale du second membre soit algébrique; car, cela fait, on égalera x à la partie réelle du second membre, y au coefficient de i, et le problème sera résolu.

D'après l'énoncé du problème, x et y ne doivent être infinies que pour $z = \pm a$, $z = \pm \alpha$; il en est donc de

même de $x+iy$ et de $x-iy$; par conséquent, le dénominateur ϖ de la quantité sous le signe $\int$ ne peut contenir que les facteurs linéaires

$$z+a,\quad z-a,\quad z+\alpha,\quad z-\alpha,$$

et il en est de même du polynôme conjugué p; d'où il suit que p contient deux de ces quatre facteurs, et que ϖ contient leurs conjugués le même nombre de fois respectivement. On peut faire quatre hypothèses :

1°. $p=(z-\alpha)^m(z+\alpha)^n,\quad \varpi=(z-a)^m(z+a)^n;$
2°. $p=(z-a)^m(z+\alpha)^n,\quad \varpi=(z-\alpha)^m(z+a)^n;$
3°. $p=(z-a)^m(z+a)^n,\quad \varpi=(z-\alpha)^m(z+\alpha)^n;$
4°. $p=(z-\alpha)^m(z+a)^n,\quad \varpi=(z-a)^m(z+\alpha)^n,$

m et n désignant des nombres entiers et positifs.

Dans la première hypothèse, on a

$$\frac{p}{\varpi}\frac{dz}{z^2-a^2}=\frac{(z-\alpha)^m(z+\alpha)^n}{(z-a)^{m+1}(z+a)^{n+1}}dz,$$

dans la seconde,

$$\frac{p}{\varpi}\frac{dz}{z^2-a^2}=\frac{(z-a)^{m-1}(z+\alpha)^n}{(z-\alpha)^m(z+a)^{n+1}}dz;$$

ou, en changeant m en $m+1$,

$$\frac{p}{\varpi}\frac{dz}{z^2-a^2}=\frac{(z-a)^m(z+\alpha)^n}{(z-\alpha)^{m+1}(z+a)^{n+1}}dz.$$

La troisième et la quatrième hypothèse donnent les mêmes valeurs de $\frac{p}{\varpi}\frac{dz}{z^2-a^2}$, sauf que a et α sont changés l'un dans l'autre, ce qui ne produit que le changement insignifiant de i en $-i$.

De tout cela, il résulte que les fonctions cherchées x

et y seront données par l'une des deux équations suivantes :

$$(5) \qquad x + iy = ce^{\omega i} \int \frac{(z-\alpha)^m (z+\alpha)^n}{(z-a)^{m+1}(z+a)^{n+1}}\, dz,$$

$$(6) \qquad x + iy = ce^{\omega i} \int \frac{(z-a)^m (z+\alpha)^n}{(z-\alpha)^{m+1}(z+a)^{n+1}}\, dz.$$

L'équation (6) est comprise dans l'équation (5), si l'on admet des valeurs négatives pour m; elle se déduit, en effet, de l'équation (5), en changeant m en $-(m+1)$.

On obtiendra la condition pour que l'intégrale de l'équation (5) soit algébrique, comme nous l'avons indiqué dans la septième leçon; mais il convient auparavant de transformer cette intégrale.

Posons

$$\frac{(a+\alpha)^2}{4a\alpha} = \zeta,$$

et prenons, à la place de z, une autre variable t, telle que

$$\frac{z+\alpha}{z+a} = \frac{2\alpha}{a+\alpha}\, t,$$

d'où

$$\frac{dz}{(z+a)^2} = \frac{2\alpha}{(a+\alpha)(a-\alpha)}\, dt;$$

on aura, après quelques réductions faciles,

$$\int \frac{(z-\alpha)^m (z+\alpha)^n}{(z-a)^{m+1}(z+a)^{n+1}}\, dz$$
$$= \frac{(2\alpha)^n (a+\alpha)^{m-n}}{(2a)^{m+1}} \int \frac{t^n (t-1)^m}{(t-\zeta)^{m+1}}\, dt.$$

Donc, pour que x et y soient algébriques, il faut et il

suffit que l'intégrale

$$(7) \qquad \int \frac{t^n (t-1)^m}{(t-\zeta)^{m+1}} dt$$

le soit. Il faut donc qu'en décomposant

$$\frac{t^n (t-1)^m}{(t-\zeta)^{m+1}}$$

en fractions simples, on ne trouve pas de terme contenant en dénominateur la première puissance de $t-\zeta$; en d'autres termes, il faut que la $m^{ième}$ dérivée de la fonction $t^n (t-1)^m$ soit nulle pour $t=\zeta$; la condition que nous cherchons est donc

$$(8) \qquad \frac{d^m \zeta^n (\zeta-1)^m}{d\zeta^m} = 0.$$

Le changement de a et α en $-a$ et $-\alpha$ dans l'intégrale (5) équivaut au changement des exposants m et n l'un dans l'autre; et comme ζ ne change pas quand on change a et α en $-a$ et $-\alpha$, il s'ensuit qu'on peut, dans la relation (8), changer m et n l'un dans l'autre. Notre équation de condition peut donc s'écrire de la manière suivante :

$$(9) \qquad \frac{d^n \zeta^m (\zeta-1)^n}{d\zeta^n} = 0.$$

Au surplus, il est aisé de s'assurer que les équations (8) et (9) sont équivalentes, car on a l'identité

$$\frac{\zeta^n}{1.2\ldots n} \frac{d^n \zeta^m (\zeta-1)^n}{d\zeta^n} = \frac{\zeta^m}{1.2\ldots m} \frac{d^m \zeta^n (\zeta-1)^m}{d\zeta^m}.$$

Les équations (8) et (9) ne diffèrent donc qu'en ce que, si m et n sont inégaux, l'une a des racines nulles. Mais les racines $\zeta=0$ ne peuvent nous convenir, car $\zeta=0$ donne $a=-\alpha$, et dans ce cas a^2 et α^2 ne sont pas imaginaires comme on l'a supposé.

Supposons que n ne soit pas inférieur à m, l'équation (9) sera du degré m, et ses m racines seront réelles et comprises entre 0 et 1. Ce théorème se démontre immédiatement, en appliquant m fois de suite le théorème de Rolle à l'équation

$$\zeta^m(\zeta-1)^n=0,$$

qui a m racines nulles et n racines égales à 1.

En désignant par ζ une racine quelconque de l'équation (9), on aura

$$(10)\qquad \frac{(a+\alpha)^2}{4a\alpha}=\zeta;$$

on pourra se donner, à volonté, le module ρ des imaginaires a et α, et si l'on pose

$$(11)\qquad a\alpha=\rho^2,$$

les équations (10) et (11) détermineront a et α, qui seront bien, en effet, imaginaires et conjuguées, à cause de $\zeta<1$.

Considérons maintenant l'équation (6); comme elle se déduit de l'équation (5) en changeant m en $-(m+1)$, on peut admettre que la condition nécessaire pour que l'intégrale qu'elle contient soit algébrique, se déduit de l'équation (9) par ce même changement. Cette condition sera donc

$$(12)\qquad \frac{d^n\dfrac{(\zeta-1)^n}{\zeta^{m+1}}}{d\zeta^n}=0.$$

Et, en faisant usage du théorème de Rolle, on voit que cette équation a toutes ses racines réelles et plus grandes que 1; en sorte que si l'on pose

$$\frac{(a+\alpha)^2}{4a\alpha}=\zeta,$$

les quantités a et α ne pourront pas être imaginaires et conjuguées.

On voit enfin que l'équation (1) ne peut admettre de solutions réelles et rationnelles que celles qui sont données par l'équation (5), où m et n représentent des nombres entiers indéterminés, et encore faut-il, pour qu'elle en admette effectivement, que la quantité

$$\zeta = \frac{(a+\alpha)^2}{4a\alpha}$$

soit une racine de l'équation (8).

Je ne parlerai point ici des applications que j'ai faites des résultats qui précèdent, et je renverrai le lecteur aux divers Mémoires que j'ai publiés sur cette question.

FIN.

NOTES.

NOTE I.

SUR LA DÉTERMINATION DES SOMMES DE PUISSANCES SEMBLABLES DES RACINES D'UNE ÉQUATION.

Formule de Lagrange.

Lagrange a fait connaître dans les *Mémoires de l'Académie de Berlin* pour 1768, et plus tard dans le *Traité de la résolution des équations numériques,* Note XI, une formule remarquable qui donne immédiatement l'expression de la somme des puissances semblables, d'un degré négatif quelconque, des racines d'une équation. La même formule peut donner aussi la somme des puissances semblables d'un degré positif; il suffira, en effet, pour avoir la valeur de cette somme, de transformer l'équation proposée en mettant au lieu de l'inconnue son inverse, et d'appliquer ensuite la formule à cette transformée. Nous allons établir ici la formule de Lagrange; nous supposerons avec l'illustre auteur que l'on ait mis l'équation dont il s'agit sous la forme

$$(1) \qquad u - x + f(x) = 0,$$

u désignant une constante et $f(x)$ étant un polynôme tel, que

$$f(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3 + \ldots,$$

dont nous représenterons la dérivée par $f'(x)$, conformément à l'usage.

On sait (*voir* première leçon) que si $a, b, c, \ldots, l$ sont les

racines de l'équation (1), la somme

$$\frac{1}{a^{n+1}}+\frac{1}{b^{n+1}}+\frac{1}{c^{n+1}}+\ldots+\frac{1}{l^{n+1}}$$

sera le coefficient de x^n dans le développement de la fonction

$$\frac{1-f'(x)}{u-x+f(x)},$$

suivant les puissances croissantes de x. Soit la fonction plus générale

$$\frac{\varphi(x)}{u-x+f(x)},$$

où $\varphi(x)$ désigne un polynôme ayant pour valeur

$$\varphi(x)=B_0+B_1x+B_2x^2+B_3x^3+\ldots,$$

et cherchons le coefficient de x^n dans le développement de cette fonction. Si l'on commence par développer suivant les puissances croissantes de $f(x)$, il vient

$$(2)\quad \frac{\varphi(x)}{u-x+f(x)}=\frac{\varphi(x)}{u-x}-\frac{\varphi(x)f(x)}{(u-x)^2}+\frac{\varphi(x)[f(x)]^2}{(u-x)^3}-\ldots$$

Considérons d'abord le premier terme du second membre, on a

$$\frac{1}{u-x}=\frac{1}{u}+\frac{x}{u^2}+\frac{x^2}{u^3}+\ldots,$$

et si l'on multiplie de part et d'autre par le polynôme $\varphi(x)$, on trouve que le coefficient de x^n dans le développement de $\frac{\varphi(x)}{u-x}$ a pour valeur

$$\frac{B_0}{u^{n+1}}+\frac{B_1}{u^n}+\frac{B_2}{u^{n-1}}+\ldots+\frac{B_n}{u},$$

ou

$$\frac{B_0+B_1u+B_2u^2+\ldots+B_nu^n}{u^{n+1}};$$

en sorte que ce coefficient pourra être représenté par

$$\frac{\varphi(u)}{u^{n+1}},$$

pourvu qu'on ne retienne que les termes qui contiennent u en dénominateur.

Considérons maintenant un terme quelconque du second membre de l'équation (2), celui qui contient la puissance i de $f(x)$ et qui a pour valeur

$$(-1)^i \frac{\varphi(x)[f(x)]^i}{(u-x)^{i+1}}.$$

D'après ce qui a été dit plus haut, le coefficient de x^n dans le développement de

$$\frac{\varphi(x)[f(x)]^i}{u-x}$$

est égal à

$$\frac{\varphi(u)[f(u)]^i}{u^{n+1}},$$

pourvu qu'on ne retienne que les termes qui contiennent u en dénominateur. On a donc, avec cette restriction,

$$\frac{\varphi(x)[f(x)]^i}{u-x} = \sum \frac{\varphi(u)[f(u)]^i}{u^{n+1}} x^n,$$

le signe $\sum$ s'étendant à toutes les valeurs entières nulles ou positives de n. Et, comme la différentiation relative à u ne peut introduire de puissances négatives de u dans les termes qui n'en contiennent pas, on aura, en prenant les dérivées d'ordre i des deux membres de l'égalité précédente,

$$1.2\ldots i(-1)^i \frac{\varphi(x)[f(x)]^i}{(u-x)^{i+1}} = \sum \frac{d^i \frac{\varphi(u)[f(u)]^i}{u^{n+1}}}{du^i} x^n,$$

d'où il suit que le coefficient de x^n dans le développement de

$$(-1)^i \frac{\varphi(x)[f(x)]^i}{(u-x)^{i+1}}$$

sera représenté par l'expression

$$\frac{1}{1.2\ldots i}\,\frac{d^i\,\dfrac{\varphi(u)[f(u)]^i}{u^{n+1}}}{du^i}$$

où il ne faut retenir que les termes qui contiennent u en dénominateur.

D'après cela, si l'on représente par

$$P_0 + P_1 x + P_2 x^2 + P_3 x^3 + \ldots,$$

le développement de la fonction

$$\frac{\varphi(x)}{u-x+f(x)},$$

on aura

$$P_n = \frac{\varphi(u)}{u^{n+1}} + \frac{d\,\dfrac{\varphi(u)f(u)}{u^{n+1}}}{du} + \frac{1}{1.2}\,\frac{d^2\,\dfrac{\varphi(u)[f(u)]^2}{u^{n+1}}}{du^2} + \ldots;$$

pourvu, nous le répétons, qu'on ne retienne que les termes qui contiennent u en dénominateur.

Supposons que la fonction $\varphi(x)$ soit de la forme

$$\varphi(x) = \psi(x)[1 - f'(x)],$$

et faisons, pour abréger,

$$\Psi(u) = \frac{\psi(u)}{u^{n+1}},$$

la valeur de P_n sera

$$P_n = \Psi(u) - \Psi(u)f'(u) + \frac{d\Psi(u)f(u)}{du} - \frac{d\Psi(u)f(u)f'(u)}{du}$$
$$+ \frac{1}{1.2}\,\frac{d^2\Psi(u)[f(u)]^2}{du^2} - \frac{1}{1.2}\,\frac{d^2\Psi(u)[f(u)]^2 f'(u)}{du^2} + \ldots$$

Or on a, en faisant $\frac{d\Psi(u)}{du} = \Psi'(u)$,

$$\frac{d\Psi(u)f(u)}{du} = \Psi(u)f'(u) + \Psi'(u)f(u);$$

on a aussi

$$\frac{1}{1.2\ldots i}\frac{d\Psi(u)[f(u)]^i}{du} = \frac{1}{1.2\ldots(i-1)}\Psi(u)[f(u)]^{i-1}f'(u)$$
$$+ \frac{1}{1.2\ldots i}\Psi'(u)[f(u)]^i,$$

et, en différentiant $i-1$ fois,

$$\frac{1}{1.2\ldots i}\frac{d^i\Psi(u)[f(u)]^i}{du^i} = \frac{1}{1.2\ldots(i-1)}\frac{d^{i-1}\Psi(u)[f(u)]^{i-1}f'(u)}{du^{i-1}}$$
$$+ \frac{1}{1.2\ldots i}\frac{d^{i-1}\Psi'(u)[f(u)]^i}{du^{i-1}};$$

au moyen de ces formules de réduction la valeur de P_n devient

$$P_n = \Psi(u) + \Psi'(u)f(u)$$
$$+ \frac{1}{1.2}\frac{d\Psi'(u)[f(u)]^2}{du} + \frac{1}{1.2.3}\frac{d^2\Psi'(u)[f(u)]^3}{du^2} + \ldots.$$

Supposons maintenant que la fonction $\psi(x)$ se réduise à l'unité; on a

$$\Psi(u) = \frac{1}{u^{n+1}};$$

d'ailleurs P_n se réduit à

$$\frac{1}{a^{n+1}} + \frac{1}{b^{n+1}} + \ldots + \frac{1}{l^{n+1}}.$$

On a donc, en mettant partout n au lieu de $n+1$ et en désignant

par $\left(\frac{1}{u^n}\right)'$ la dérivée de $\frac{1}{u^n}$,

$$\frac{1}{a^n}+\frac{1}{b^n}+\frac{1}{c^n}+\ldots+\frac{1}{l^n}=\frac{1}{u^n}+\left(\frac{1}{u^n}\right)'f(u)$$
$$+\frac{1}{1.2}\frac{d\left(\frac{1}{u^n}\right)'[f(u)]^2}{du}+\frac{1}{1.2.3}\frac{d^2\left(\frac{1}{u^n}\right)'[f(u)]^3}{du^2}+\ldots,$$

où l'on ne doit retenir que les termes qui contiennent u en dénominateur.

Lagrange a tiré de la formule précédente des conséquences importantes; il en a déduit en particulier la formule remarquable que nous avons établie dans la vingt-neuvième leçon. Nous renvoyons pour ces développements au *Traité de la résolution des équations numériques*.

Formule de Waring.

Appliquons ce qui précède à la recherche de la somme des puissances semblables d'un degré entier et positif n des racines de l'équation

$$(1)\qquad x^m+p_1x^{m-1}+p_2x^{m-2}+\ldots+p_{m-1}x+p_m=0.$$

Nous désignerons par $a, b, c, \ldots, l$ les racines de cette équation, et nous poserons

$$s_n=a^n+b^n+c^n+\ldots+l^n.$$

Si l'on change x en $\frac{1}{x}$, l'équation proposée devient

$$(2)\qquad -\frac{1}{p_1}-x-\left(\frac{p_2}{p_1}x^2+\frac{p_3}{p_1}x^3+\ldots+\frac{p_m}{p_1}x^m\right)=0,$$

ou

$$u-x+f(x)=0,$$

en mettant u au lieu de $-\frac{1}{p_1}$, dans le premier terme, et en

faisant

$$f(x) = -\left(\frac{p_2}{p_1}x^2 + \frac{p_3}{p_1}x^3 + \ldots + \frac{p_m}{p_1}x^m\right).$$

Or les racines de l'équation (2) sont les inverses de celles de l'équation (1); on aura donc, d'après le théorème de Lagrange,

$$(3)\left\{\begin{aligned} s_n = {} & \frac{1}{u^n} - n\frac{1}{u^{n+1}}f(u) \\ & - \frac{n}{1.2}\,\frac{d\,\frac{1}{u^{n+1}}[f(u)]^2}{du} - \frac{n}{1.2.3}\,\frac{d^2\,\frac{1}{u^{n+1}}[f(u)]^3}{du^2} - \ldots, \end{aligned}\right.$$

formule dont le terme général est

$$(4) \qquad -\frac{n}{1\;2\;3\ldots i}\,\frac{d^{i-1}\frac{1}{u^{n+1}}[f(u)]^i}{du^{i-1}},$$

et où il faut retenir seulement les termes qui contiennent u en dénominateur. Cherchons à quoi se réduit l'expression (4).

Conformément à l'usage adopté par plusieurs géomètres, nous conviendrons que le symbole $\Gamma(\mu+1)$ représentera le produit des μ premiers nombres entiers dans le cas de μ entier positif, et que le même symbole se réduira à l'unité dans le cas de $\mu = 0$; ainsi l'on aura

$$\Gamma(\mu+1) = 1.2.3\ldots\mu \quad \text{et} \quad \Gamma(1) = 1.$$

Cela posé, on a

$$f(u) = -\left(\frac{p_2}{p_1}u^2 + \frac{p_3}{p_1}u^3 + \ldots + \frac{p_m}{p_1}u^m\right),$$

et, en élevant à la puissance i,

$$[f(u)]^i = (-1)^i \sum \frac{\Gamma(i+1)}{\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_m+1)}\,\frac{p_2^{\lambda_2}\ldots p_m^{\lambda_m}}{p_1^{\lambda_2+\ldots+\lambda_m}}\,u^{2\lambda_2+\ldots+m\lambda_m};$$

le signe sommatoire $\sum$ s'etend à toutes les valeurs entières positives ou nulles des exposants $\lambda_2, \lambda_3, \ldots, \lambda_m$, assujettis seule-

ment à vérifier l'équation de condition

$$(5) \qquad \lambda_2 + \lambda_3 + \ldots + \lambda_m = i.$$

Si l'on multiplie cette valeur de $[f(u)]^i$ par $\frac{-nu^{-n-1}}{\Gamma(i+1)}$, et qu'on détermine le nombre λ_1 par la condition

$$(6) \qquad \lambda_1 + 2\lambda_2 + 3\lambda_3 \ldots + m\lambda_m = n,$$

il viendra

$$-\frac{n}{1.2\ldots i}\frac{1}{u^{n+1}}[f(u)]^i$$

$$= (-1)^{i-1}\sum \frac{n}{\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_m+1)}\frac{p_2^{\lambda_2}\ldots p_m^{\lambda_m}}{p_1^{\lambda_2+\ldots+\lambda_m}}u^{-(\lambda_1+1)},$$

et comme nous n'avons à tenir compte, dans le second membre, que des termes qui contiennent u en dénominateur, on voit que le nombre λ_1 ne devra recevoir aucune valeur négative. Si l'on prend les dérivées d'ordre $i-1$, par rapport à u, des deux membres de l'égalité précédente, il vient, en ayant égard à la condition (5),

$$(7)\quad \left\{ \begin{aligned} & -\frac{n}{1.2\ldots i}\frac{d^{i-1}\frac{1}{u^{n+1}}[f(u)]^i}{du^{i-1}} \\ & = \sum \frac{n\,\Gamma(\lambda_1+\lambda_2+\ldots\lambda_m)}{\Gamma(\lambda_1+1)\ldots\Gamma(\lambda_m+1)}\frac{p_2^{\lambda_2}\ldots p_m^{\lambda_m}}{p_1^{\lambda_2+\ldots+\lambda_m}}\frac{1}{u^{\lambda_1+\ldots+\lambda_m}}. \end{aligned} \right.$$

Le second membre de cette équation (7) exprime la somme des termes du premier membre qui contiennent u en dénominateur; ces termes sont les seuls qu'il faille retenir; le signe $\sum$ s'étend à toutes les valeurs entières nulles ou positives des exposants $\lambda_1, \lambda_2, \ldots, \lambda_m$ susceptibles de vérifier les équations de condition (5) et (6). En faisant successivement

$$i = 2, 3, 4, \ldots,$$

l'équation (7) fera connaître la partie à conserver dans les dif-

férents termes du second membre de l'équation (3), à partir du troisième. Mais je dis, de plus, que le second membre de l'équation (7) exprimera pour $i=1$, la partie à conserver dans le deuxième terme de la valeur de s_n, et que pour $i=0$, ce même second membre se réduira au premier terme $\frac{1}{u_n}$ de la valeur de s_n. En effet, pour $i=1$, les exposants $\lambda_2, \lambda_3, \ldots, \lambda_m$ sont nuls, à l'exception de l'un d'eux, qui est égal à 1; si c'est λ_ρ qui est égal à 1, λ_1 est égal à $n-\rho$ d'après la condition (6); le second membre de l'équation (7) se réduit alors à

$$n \sum \frac{p_\rho}{p_1} \frac{1}{u^{n+1-\rho}},$$

où le signe $\sum$ s'étend aux valeurs de ρ depuis $\rho=2$ jusqu'à $\rho=m$ si m est moindre que n, et jusqu'à $\rho=n$ si m est plus grand que n. On voit que l'expression précédente représente la somme des termes de $-n\frac{1}{u^{n+1}}f(u)$, qui contiennent u en dénominateur.

Enfin, pour $i=0$, les exposants $\lambda_2, \lambda_3, \ldots, \lambda_m$ sont tous nuls, et λ_1 se réduit à n à cause de la relation (6); et, à cause de $n\Gamma(n)=\Gamma(n+1)$, on voit que le second membre de l'équation (7) se réduit au terme unique $\frac{1}{u^n}$, qui est le premier terme du second membre de l'équation (3).

Le second membre de l'équation (7) ne renferme pas explicitement l'indice i; donc, d'après ce qui précède, ce second membre exprimera la partie à conserver dans les différents termes qui composent le second membre de l'équation (3), pourvu que l'on fasse abstraction de la condition (5) et qu'on n'ait égard qu'à la condition (6). Ainsi l'on a

$$s_n = \sum \frac{n\Gamma(\lambda_1+\lambda_2+\ldots+\lambda_m)}{\Gamma(\lambda_1+1)\ldots\Gamma(\lambda_m+1)} \frac{p_2^{\lambda_2}\ldots p_m^{\lambda_m}}{p_1^{\lambda_1+\ldots+\lambda_m}} \frac{1}{u^{\lambda_1+\ldots+\lambda_m}},$$

ou, en remettant $-\frac{1}{p_1}$ au lieu de u,

$$(8)\quad s_n = \sum \frac{(-1)^{\lambda_1+\lambda_2+\ldots+\lambda_m} n\,\Gamma(\lambda_1+\lambda_2+\ldots+\lambda_m)}{\Gamma(\lambda_1+1)\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_m+1)} p_1^{\lambda_1} p_2^{\lambda_2}\ldots p_m^{\lambda_m},$$

le signe $\sum$ s'etendant, nous le répétons, à toutes les valeurs entières nulles et positives des exposants $\lambda_1, \lambda_2, \ldots, \lambda_m$ susceptibles de vérifier la condition

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots + m\lambda_m = n.$$

La formule (8) fait ainsi connaître immédiatement, en fonction des coefficients, la somme des puissances $n^{\text{ièmes}}$ des racines d'une équation ; elle a été donnée par Waring, dans ses *Meditationes algebraïcæ* (*). Waring ne fait pas connaître la méthode qui l'a conduit à sa formule, il se borne à en vérifier l'exactitude à posteriori.

Application de la formule de Waring à l'équation du second degré.

Écrivons l'équation du second degré sous la forme

$$x^2 - px + q = 0.$$

Pour avoir la somme des puissances $n^{\text{ièmes}}$ des racines, il faudra faire, dans la formule (8) de Waring,

$$p_1 = -p, \quad p_m = p_2 = q;$$

si l'on pose, en outre, $\lambda_2 = \mu$, on aura $\lambda_1 = n - 2\mu$. On trouve alors cette valeur de s_n,

$$s_n = \sum \frac{(-1)^{\mu} n\,\Gamma(n-\mu)}{\Gamma(n-2\mu+1)\Gamma(\mu+1)} p^{n-2\mu} q^{\mu},$$

le signe $\sum$ s'étendant aux valeurs de μ

$$0,\ 1,\ 2,\ldots,$$

(*) *Editio tertia*, p. 1.

jusqu'au plus grand entier contenu dans $\frac{n}{2}$ En remplaçant les Γ par leurs valeurs, il vient

$$s_n = p^n - np^{n-2}q + \frac{n(n-3)}{1.2}p^{n-4}q^2 - \ldots$$
$$+ (-1)^\mu \frac{n(n-\mu-1)(n-\mu-2)\ldots(n-2\mu+1)}{1.2\ldots\mu}p^{n-2\mu}q^\mu + \ldots$$

On déduit immédiatement de cette formule la valeur du polynôme V_n que nous avons étudié dans la quatorzième leçon. En effet, V_n est une fonction entière de z définie par les deux équations

$$V_n = x^n + \frac{1}{x^n}, \quad x + \frac{1}{x} = z.$$

Il s'ensuit que V_n est la somme des puissances $n^{i\grave{e}mes}$ des racines de l'équation

$$(t-x)\left(t-\frac{1}{x}\right) = 0, \quad \text{ou} \quad t^2 - zt + 1 = 0,$$

par conséquent la valeur de V_n se déduira de celle de s_n écrite plus haut, en faisant $p = z$ et $q = 1$; il vient ainsi

$$V_n = z^n - nz^{n-2} + \frac{n(n-3)}{1.2}z^{n-4} - \ldots$$
$$+ (-1)^\mu \frac{n(n-\mu-1)\ldots(n-2\mu+1)}{1.2\ldots\mu}z^{n-2\mu} + \ldots,$$

formule qui coïncide avec celle que nous avons donnée dans la quatorzième leçon et que nous avons déduite d'une analyse toute différente.

NOTE II.

SUR L'EXPRESSION D'UNE FONCTION SYMÉTRIQUE D'ORDRE QUELCONQUE DES RACINES D'UNE ÉQUATION, EN FONCTION DES SOMMES DE PUISSANCES SEMBLABLES DES RACINES.

Formule de Waring.

Waring a donné, dans ses *Meditationes algebraicæ* (*), une formule qui fait connaître l'expression d'une fonction symétrique d'ordre quelconque des racines d'une équation, en fonction des sommes de puissances semblables des racines. Nous allons établir ici cette formule remarquable.

Soient

$$x_1,\ x_2, \ldots,\ x_m$$

les m racines d'une équation de degré m, et

$$\alpha_1,\ \alpha_2, \ldots,\ \alpha_i,$$

des entiers positifs ou négatifs.

Nous conserverons la notation dont nous avons fait usage dans la première leçon, en sorte que S_{α_i} représentera la somme des puissances de degré α_i de toutes les racines, et que le symbole

$$\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_i^{\alpha_i}$$

désignera la fonction symétrique d'ordre i, dont tous les termes se déduisent de $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_i^{\alpha_i}$, en faisant toutes les permutations possibles des racines. Nous supposerons d'abord que les exposants α soient inégaux, et alors on aura

$$(1)\quad \left\{\begin{aligned} &\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_i^{\alpha_i} = S_{\alpha_i} \sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{i-1}^{\alpha_{i-1}} \\ &- \sum x_1^{\alpha_1+\alpha_i} x_2^{\alpha_2} \ldots x_{i-1}^{\alpha_{i-1}} - \sum x_1^{\alpha_1} x_2^{\alpha_2+\alpha_i} \ldots x_{i-1}^{\alpha_{i-1}} \ldots \\ &- \sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{i-1}^{\alpha_{i-1}+\alpha_i}. \end{aligned}\right.$$

(*) *Editio tertia*, p. 8

Cette formule permet de calculer les fonctions symétriques d'ordre i quand on sait former celles de l'ordre $i-1$; on en déduit :

$$\sum x_1^{\alpha_1} x_2^{\alpha_2} = S_{\alpha_1} S_{\alpha_2} - S_{\alpha_1+\alpha_2},$$

$$\sum x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} = S_{\alpha_1} S_{\alpha_2} S_{\alpha_3}$$
$$-(S_{\alpha_1} S_{\alpha_2+\alpha_3} + S_{\alpha_2} S_{\alpha_1+\alpha_3} + S_{\alpha_3} S_{\alpha_1+\alpha_2}) + 2 S_{\alpha_1+\alpha_2+\alpha_3},$$

$$\sum x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} = S_{\alpha_1} S_{\alpha_2} S_{\alpha_3} S_{\alpha_4}$$
$$-\left(\begin{array}{l} S_{\alpha_1} S_{\alpha_2} S_{\alpha_3+\alpha_4} + S_{\alpha_1} S_{\alpha_3} S_{\alpha_2+\alpha_4} + S_{\alpha_1} S_{\alpha_4} S_{\alpha_2+\alpha_3} \\ + S_{\alpha_2} S_{\alpha_3} S_{\alpha_1+\alpha_4} + S_{\alpha_2} S_{\alpha_4} S_{\alpha_1+\alpha_3} + S_{\alpha_3} S_{\alpha_4} S_{\alpha_1+\alpha_2} \end{array}\right)$$
$$+2\left(\begin{array}{l} S_{\alpha_1} S_{\alpha_2+\alpha_3+\alpha_4} + S_{\alpha_2} S_{\alpha_4+\alpha_3+\alpha_1} \\ + S_{\alpha_3} S_{\alpha_1+\alpha_2+\alpha_4} + S_{\alpha_4} S_{\alpha_1+\alpha_2+\alpha_3} \end{array}\right)$$
$$+(S_{\alpha_1+\alpha_2} S_{\alpha_3+\alpha_4} + S_{\alpha_1+\alpha_3} S_{\alpha_2+\alpha_4} + S_{\alpha_1+\alpha_4} S_{\alpha_2+\alpha_3})$$
$$-2.3 S_{\alpha_1+\alpha_2+\alpha_3+\alpha_4},$$

....
....

On peut écrire ces formules d'une manière plus abrégée et découvrir la loi de leur formation en faisant usage de la notation suivante : partageons les i indices

$$\alpha_1, \alpha_2, \ldots, \alpha_i$$

en divers groupes. Soient λ_1 le nombre des groupes qui contiennent un seul indice, λ_2 le nombre des groupes qui contiennent deux indices, ..., λ_i le nombre des groupes qui contiennent i indices; on aura

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots + i\lambda_i = i;$$

on voit que λ_i doit être égal à zéro ou à l'unité, et si $\lambda_i = 1$, tous les autres λ sont nuls. Cela posé, ajoutons entre eux les indices α de chaque groupe et désignons par

$$6_1, 6_2, \ldots, 6_\mu$$

les sommes obtenues; enfin considérons le produit

$$S_{\varepsilon_1} S_{\varepsilon_2} \dots S_{\varepsilon_\mu},$$

faisons toutes les permutations des indices $\alpha_1, \alpha_2, \dots, \alpha_i$ qui font acquérir à ce produit toutes les valeurs distinctes dont il est susceptible, ajoutons tous les résultats et désignons par

$$T(\lambda_1, \lambda_2, \dots, \lambda_i)$$

la somme obtenue qui sera une fonction symétrique des indices α.

D'après cette notation, les formules écrites plus haut deviennent

$$(2)\quad \left\{\begin{aligned}
&\sum x_1^{\alpha_1} x_2^{\alpha_2} = T(2,0) - T(0,1),\\
&\sum x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} = T(3,0,0) - T(1,1,0) + 2T(0,0,1),\\
&\sum x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} = T(4,0,0,0) - T(2,1,0,0)\\
&\qquad\qquad + 2T(1,0,1,0) - 2.3\,T(0,0,0,1),\\
&\sum x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} x_5^{\alpha_5} = T(5,0,0,0,0) - T(3,1,0,0,0),\\
&\qquad\qquad + 2T(2,0,1,0,0) + T(1,2,0,0,0)\\
&\qquad\qquad - 2.3\,T(1,0,0,1,0) - 2T(0,1,1,0,0)\\
&\qquad\qquad + 2.3.4\,T(0,0,0,0,1),\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots
\end{aligned}\right.$$

et il est aisé de vérifier qu'on a généralement

$$(3)\quad \left\{\begin{aligned}
&\sum x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \dots x_i^{\alpha_i}\\
&= \sum (-1)^{i-\lambda_1-\lambda_2-\dots-\lambda_i}\,\Gamma(2)^{\lambda_2}\Gamma(3)^{\lambda_3}\dots\Gamma(i)^{\lambda_i}\,T(\lambda_1, \lambda_2, \dots, \lambda_i),
\end{aligned}\right.$$

le signe $\sum$ du second membre s'étendant à toutes les valeurs de $\lambda_1, \lambda_2, \ldots, \lambda_i$, qui satisfont à la condition

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots + i\lambda_i = i,$$

et le symbole $\Gamma(\mu)$ désignant, comme dans la Note I, le produit des $\mu - 1$ premiers nombres entiers.

Au moyen des formules (2) on vérifie l'exactitude de la formule (3) pour $i = 2, 3, 4, 5$; donc, pour établir la généralité de celle-ci, il suffit de prouver que si elle a lieu pour $i = k$, elle a lieu aussi pour $i = k + 1$. Admettons donc que l'on ait

$$(4)\quad \left\{ \begin{aligned} &\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} \\ &= \sum (-1)^{k-\lambda_1-\lambda_2-\ldots-\lambda_k} \Gamma(2)^{\lambda_2} \Gamma(3)^{\lambda_3} \ldots \Gamma(k)^{\lambda_k} \mathrm{T}(\lambda_1, \lambda_2, \ldots, \lambda_k), \end{aligned} \right.$$

le signe $\sum$ du second membre s'étendant à toutes les valeurs des entiers λ, pour lesquelles on a

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots + k\lambda_k = k.$$

Il est évident que l'expression de

$$\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}}$$

sera formée de termes tels que

$$\mathrm{T}(\lambda_1, \lambda_2, \ldots, \lambda_k, \lambda_{k+1});$$

où l'on aura

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots + k\lambda_k + (k+1)\lambda_{k+1} = k + 1;$$

nous allons chercher à déterminer les coefficients qui multiplient ces différents termes.

Supposons d'abord que λ_1 ne soit pas nul, ce qui exige que λ_{k+1} le soit; on aura

$$(\lambda_1 - 1) + 2\lambda_2 + 3\lambda_3 + \ldots + k\lambda_k = k.$$

Cela posé, le terme en

$$T(\lambda_1, \lambda_2, \ldots, \lambda_k, 0),$$

que nous considérons, proviendra en partie [formule (1)] de la multiplication de $S_{\alpha_{k+1}}$ par $\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$, et comme les termes de ce produit ne peuvent évidemment se réduire avec ceux qui proviennent du changement de α_1 en $\alpha_1 + \alpha_{k+1}$, ou de α_2 en $\alpha_2 + \alpha_{k+1}$, ou, etc., il est clair que le coefficient de

$$T(\lambda_1, \lambda_2, \ldots, \lambda_k, 0)$$

dans $\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{k+1}^{\alpha_{k+1}}$ sera égal au coefficient de

$$T(\lambda_1 - 1, \lambda_2, \ldots, \lambda_k)$$

dans $\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$, c'est-à-dire égal à

$$(-1)^{k+1-\lambda_1-\lambda_2-\ldots-\lambda_k} \Gamma(2)^{\lambda_2} \Gamma(3)^{\lambda_3} \ldots \Gamma(k)^{\lambda_k};$$

ce résultat est conforme à celui qu'on déduit de la formule (3) quand on y fait $i = k + 1$.

Considérons maintenant le terme en

$$T(0, \lambda_2, \ldots, \lambda_g, \lambda_{g+1}, \ldots, \lambda_k, 0),$$

dans $\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}}$. Ce terme provient tout entier [formule (1)] des résultats que l'on obtient en changeant, dans $-\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$, α_1 en $\alpha_1 + \alpha_{k+1}$, ou α_2 en $\alpha_2 + \alpha_{k+2}$, ou, etc.

Les termes de l'expression (4) de $-\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$ qui concourent ainsi à former le terme que nous considérons sont évidemment de la forme

$$T(0, \lambda_2, \ldots, \lambda_g + 1, \lambda_{g+1} - 1, \ldots, \lambda_k),$$

où g peut avoir toutes les valeurs telles, que λ_{g+1} ne soit pas nul,

et le coefficient correspondant sera, d'après la formule (4),

$$(-1)^{k+1-\lambda_2-\lambda_3-\ldots-\lambda_k}\Gamma(2)^{\lambda_2}\Gamma(3)^{\lambda_3}\ldots\Gamma(g)^{\lambda_g+1}\Gamma(g+1)^{\lambda_{g+1}-1}\ldots\Gamma(k)^{\lambda_k}.$$

Or, chacun des termes de

$$T(0,\lambda_2,\ldots,\lambda_g+1,\ \lambda_{g+1}-1,\ldots,\lambda_k)$$

contient, d'après sa définition même, un ou plusieurs facteurs de la forme

$$S_{\alpha_1+\alpha_2+\ldots},$$

où le nombre des indices α est égal à g; si, dans les facteurs de ce genre, on remplace successivement α_1 par $\alpha_1+\alpha_{k+1}$, puis α_2 par $\alpha_2+\alpha_{k+1}$, puis, etc., et qu'on réunisse ensuite tous les résultats, chaque terme sera répété g fois dans la somme. Il s'ensuit que le terme en

$$T(0,\lambda_2,\ldots,\lambda_g+1,\lambda_{g+1}-1,\ldots,\lambda_k)$$

donnera, dans $\sum x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_k^{\alpha_k}x_{k+1}^{\alpha_{k+1}}$, une partie des termes contenus dans l'expression

$$T(0,\lambda_2,\ldots,\lambda_g,\lambda_{g+1},\ldots\lambda_k,0),$$

et que ceux-ci auront pour coefficient

$$g(-1)^{k+1-\lambda_2-\lambda_3-\ldots-\lambda_k}\Gamma(2)^{\lambda_2}\ldots\Gamma(g)^{\lambda_g+1}\Gamma(g+1)^{\lambda_{g+1}-1}\ldots\Gamma(k)^{\lambda_k},$$

ou

$$(-1)^{k+1-\lambda_2-\lambda_3-\ldots-\lambda_k}\Gamma(2)^{\lambda_2}\ldots\Gamma(g)^{\lambda_g}\Gamma(g+1)^{\lambda_{g+1}}\ldots\Gamma(k)^{\lambda_k},$$

à cause de $g\Gamma(g)=\Gamma(g+1)$. Or les termes qui peuvent naître des diverses valeurs dont g est susceptible, ne peuvent se réduire entre eux; donc le coefficient de

$$T(0,\lambda_2,\lambda_3,\ldots,\lambda_k,0)$$

dans $\sum x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_k^{\alpha_k}x_{k+1}^{\alpha_{k+1}}$ est nécessairement

$$(-1)^{k+1-\lambda_2-\ldots-\lambda_k}\Gamma(2)^{\lambda_2}\Gamma(3)^{\lambda_3}\ldots\Gamma(k)^{\lambda_k}.$$

Ce résultat est conforme à celui qu'on déduit de la formule (3) en y faisant $i = k + 1$.

Considérons enfin le terme en

$$T(0,\ 0,\ 0, \ldots,\ 0,\ 1)$$

dans $\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}}$. Il se forme au moyen du seul terme

$$(-1)^k \Gamma(k)\, T(0,\ 0,\ 0, \ldots,\ 0,\ 1)$$

de $-\sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_k^{\alpha_k}$. Il faut effectivement, pour cela, ajouter successivement α_{k+1} à chacun des indices qui entrent dans ce terme, et réunir tous les k résultats qui sont évidemment égaux entre eux. On voit alors, à cause de $k\Gamma(k) = \Gamma(k+1)$, que le terme considéré a pour valeur

$$(-1)^k \Gamma(k+1)\, T(0, 0, 0, \ldots, 0, 1),$$

ce qui achève de démontrer l'exactitude de la formule (3).

Il est aisé de trouver le nombre N des termes contenus dans la fonction que nous avons désignée par

$$T(\lambda_1, \lambda_2, \ldots, \lambda_i).$$

Effectivement chacun de ces termes correspond à une certaine distribution des indices

$$\alpha_1, \alpha_2, \ldots, \alpha_i$$

en $\lambda_1 + \lambda_2 + \ldots + \lambda_i$ groupes, et λ_k désigne généralement le nombre des groupes qui renferment k indices. Écrivons, sur une même ligne, tous les indices α de manière que ceux qui appartiennent à un même groupe se trouvent placés à côté les uns des autres, en commençant par les groupes d'une seule lettre, mettant ensuite les groupes de deux lettres, et ainsi de suite. On pourra former, de cette manière, N permutations ou arrangements des i indices qui correspondront respectivement aux N termes de T. Si maintenant on fait dans chacun de ces N arrangements toutes les permutations possibles des indices qui com-

posent chaque groupe, sans altérer l'ordre des groupes et sans faire passer aucun indice d'un groupe à un autre, le nombre total des arrangements qu'on obtiendra sera égal à

$$\mathrm{N}\,\Gamma(2)^{\lambda_1}\,\Gamma(3)^{\lambda_2}\ldots\Gamma(i)^{\lambda_{i-1}}\,\Gamma(i+1)^{\lambda_i}.$$

Enfin, si dans chacun des arrangements ainsi formés, on permute entre eux, de toutes les manières possibles, d'abord les λ_1 groupes qui contiennent chacun un indice, puis les λ_2 groupes qui contiennent deux indices, puis, etc., sans altérer l'ordre des indices qui composent un même groupe, le nombre de tous les arrangements ainsi obtenus sera

$$\mathrm{N}\,\Gamma(2)^{\lambda_1}\,\Gamma(3)^{\lambda_2}\ldots\Gamma(i+1)^{\lambda_i}\,\Gamma(\lambda_1+1)\,\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_i+1).$$

Or il est évident qu'en opérant ainsi on a formé toutes les $\Gamma(i+1)$ permutations des i indices sans en omettre ou en répéter aucun. Le nombre précédent est donc égal à $\Gamma(i+1)$, et, par suite, on a

$$\mathrm{N}=\frac{\Gamma(i+1)}{\Gamma(2)^{\lambda_1}\,\Gamma(3)^{\lambda_2}\ldots\Gamma(i+1)^{\lambda_i}\,\Gamma(\lambda_1+1)\,\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_i+1)}.$$

La formule (3) suppose que les i indices

$$\alpha_1,\ \alpha_2,\ldots,\ \alpha_i$$

soient inégaux. Supposons maintenant que parmi ces indices, il y en ait μ_1 égaux à α_1, μ_2 égaux à $\alpha_2,\ldots$, enfin μ_k égaux à α_k; il est évident que le second membre de la formule (3) devra être divisé par

$$\Gamma(\mu_1+1)\,\Gamma(\mu_2+1)\ldots\Gamma(\mu_k+1),$$

ainsi que nous l'avons dit dans la première leçon.

Supposons, en particulier, que les i indices soient égaux à un même nombre α, on devra diviser le second membre de l'équation (3) par $\Gamma(i+1)$; d'ailleurs, chacun des N termes de

$$\mathrm{T}(\lambda_1,\lambda_2,\ldots,\lambda_i)$$

se réduit à

$$\mathrm{S}_{\alpha}^{\lambda_1}\,\mathrm{S}_{2\alpha}^{\lambda_2}\ldots\mathrm{S}_{i\alpha}^{\lambda_i},$$

donc cette fonction a pour valeur

$$\frac{\Gamma(i+1)}{\Gamma(2)^{\lambda_1}\Gamma(3)^{\lambda_2}\ldots\Gamma(i+1)^{\lambda_i}\Gamma(\lambda_1+1)\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_i+1)} S_\alpha^{\lambda_1} S_{2\alpha}^{\lambda_2}\ldots S_{i\alpha}^{\lambda_i},$$

ou

$$\frac{\Gamma(i+1)}{1^{\lambda_1}.2^{\lambda_2}\ldots i^{\lambda_i}\Gamma(2)^{\lambda_2}\Gamma(3)^{\lambda_3}\ldots\Gamma(i)^{\lambda_i}\Gamma(\lambda_1+1)\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_i+1)} S_\alpha^{\lambda_1} S_{2\alpha}^{\lambda_2}\ldots S_{i\alpha}^{\lambda_i};$$

la formule (3) donne alors

$$(5)\quad \begin{cases} \sum (x_1 x_2 \ldots x_i)^\alpha \\ = \sum \dfrac{(-1)^{i-\lambda_1-\lambda_2-\ldots-\lambda_i}}{1^{\lambda_1}.2^{\lambda_2}\ldots i^{\lambda_i}\Gamma(\lambda_1+1)\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_i+1)} S_\alpha^{\lambda_1} S_{2\alpha}^{\lambda_2}\ldots S_{i\alpha}^{\lambda_i}, \end{cases}$$

le signe $\sum$ du second membre s'étendant, comme précédemment, aux valeurs nulles ou positives des entiers $\lambda_1, \lambda_2, \ldots, \lambda_i$ susceptibles de vérifier la condition

$$\lambda_1 + 2\lambda_2 + \ldots + i\lambda_i = i.$$

Détermination des coefficients d'une équation en fonction des sommes de puissances semblables des racines.

La formule (5) donne immédiatement l'expression des coefficients d'une équation en fonction des sommes de puissances semblables des racines.

Soit l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

et représentons, comme précédemment, par

$$x_1,\ x_2, \ldots,\ x_m$$

ses m racines. On a

$$p_i = (-1)^i \sum x_1 x_2 \ldots x_i;$$

par suite, la formule (5) donne, en y faisant $\alpha = 1$,

$$p_i = \sum \frac{(-1)^{\lambda_1+\lambda_2+\ldots+\lambda_i}}{1^{\lambda_1}.2^{\lambda_2}.3^{\lambda_3}\ldots i^{\lambda_i}\Gamma(\lambda_1+1)\Gamma(\lambda_2+1)\ldots\Gamma(\lambda_i+1)} S_1^{\lambda_1} S_2^{\lambda_2}\ldots S_i^{\lambda_i},$$

le signe $\sum$ s'étendant toujours aux valeurs nulles et positives des exposants λ qui vérifient la condition

$$\lambda_1 + 2\lambda_2 + \ldots + i\lambda_i = i.$$

En faisant $i = 1, 2, 3, 4$, etc., on trouve

$$p_1 = -S_1,$$

$$p_2 = \frac{1}{2} S_1^2 - \frac{1}{2} S_2,$$

$$p_3 = -\frac{1}{2.3} S_1^3 + \frac{1}{2} S_1 S_2 - \frac{1}{3} S_3,$$

$$p_4 = \frac{1}{2.3.4} S_1^4 - \frac{1}{2.2} S_1^2 S_2 + \frac{1}{3} S_1 S_3 + \frac{1}{2^2.2} S_2^2 - \frac{1}{4} S_4,$$

. . . .

. . . .

Il est aisé de vérifier ces résultats au moyen des formules de Newton.

NOTE III.

SUR LA DÉTERMINATION DU DERNIER TERME DE L'ÉQUATION AUX CARRÉS DES DIFFÉRENCES.

Le produit des carrés des différences des racines d'une équation prises deux à deux, ou, ce qui revient au même, le *dernier terme de l'équation aux carrés des différences*, est une fonction entière des coefficients de l'équation proposée, qui possède plusieurs propriétés remarquables et qu'on a occasion de considérer dans diverses questions d'analyse supérieure. Nous avons fait connaître, dans la deuxième leçon, le procédé de M. Cauchy, par lequel on peut calculer la fonction dont il s'agit, pour une équation du degré m, lorsqu'on connaît la valeur de cette même fonction pour une équation de degré $m-1$. Je me propose, dans cette Note, d'indiquer un procédé nouveau et d'une grande simplicité pour résoudre la même question.

Soit l'équation de degré m,

$$(1)\quad x^m + p_1 x^{m-1} + p_2 x^{m-2} + p_3 x^{m-3} + \ldots + p_{m-1} x + p_m = 0,$$

et désignons par V_m le dernier terme de l'équation aux carrés des différences des racines. Il résulte de la théorie des fonctions symétriques, que V_m est une fonction entière des coefficients $p_1, p_2, \ldots, p_m$, et que chacun des termes de cette fonction renfermera $m(m-1)$ dimensions, si l'on considère chaque coefficient p comme ayant autant de dimensions que son indice contient d'unités. D'après cela, la valeur de V_m ordonnée par rapport aux puissances décroissantes de p_m aura la forme

$$(2)\quad V_m = A_1 p_m^{m-1} + A_2 p_m^{m-2} + A_3 p_m^{m-3} + \ldots + A_{m-1} p_m + A_m,$$

$A_1, A_2, \ldots, A_m$ étant des fonctions entières de $p_1, p_2, \ldots, p_{m-1}$ dont la première est une simple constante.

Désignons par V_{m-1} le dernier terme de l'équation aux carrés de différences des racines de l'équation

$$(3) \quad x^{m-1}+p_1 x^{m-2}+p_2 x^{m-3}+\ldots+p_{m-2} x+p_{m-1}=0.$$

Lorsque p_m est nul, la fonction V_m se réduit à A_m; d'un autre côté, l'équation (1) se déduit alors de l'équation (3) en multipliant celle-ci par x, c'est-à-dire en y introduisant une racine nulle. Il s'ensuit évidemment que l'on a

$$A_m = p_{m-1}^2 V_{m-1}.$$

Cela posé, il est évident que la fonction V_m ne changera pas, si l'on augmente chaque racine de l'équation (1) d'une même quantité h; or, par ce changement, les coefficients $p_1, p_2, \ldots, p_m$ prennent des accroissements

$$\Delta p_1, \Delta p_2, \ldots, \Delta p_{m-1}, \Delta p_m$$

qui s'évanouissent avec h, et dont les termes qui contiennent h à la première puissance, sont respectivement

$$mh, \quad (m-1)p_1 h, \quad (m-2)p_2 h, \ldots, \quad 2p_{m-2}h, \quad p_{m-1}h.$$

L'accroissement correspondant ΔV_m de V_m, savoir :

$$\Delta V_m = \frac{dV_m}{dp_1}\Delta p_1 + \frac{dV_m}{dp_2}\Delta p_2 + \ldots + \frac{dV_m}{dp_m}\Delta p_m + \ldots$$

est nul, quel que soit h, et, par conséquent, le coefficient de la première puissance de h est identiquement nul; on a donc

$$m\frac{dV_m}{dp_1} + (m-1)p_1\frac{dV_m}{dp_2} + (m-2)p_2\frac{dV_m}{dp_3} + \ldots + p_{m-1}\frac{dV_m}{dp_m} = 0.$$

On peut obtenir, d'une autre manière, cette équation qui va nous conduire à la valeur de V_m. Si, en effet, on fait disparaître le second terme de l'équation (1) et qu'on exprime, par le moyen des différentielles partielles, que V_m est une fonction des coefficients de l'équation transformée, on retrouvera l'équation que nous venons de former. Nous écri-

rons, pour abréger, cette équation de la manière suivante :

$$\frac{dV_m}{d\zeta} = 0,$$

en feignant que $p_1, p_2, \ldots, p_m$ soient des fonctions d'une variable ζ, qui aient respectivement pour dérivées

$$\frac{dp_1}{d\zeta} = m,\ \frac{dp_2}{d\zeta} = (m-1)p_1, \ldots,\ \frac{dp_{m-1}}{d\zeta} = 2p_{m-2},\ \frac{dp_m}{d\zeta} = p_{m-1}.$$

En différentiant l'équation (2) par rapport à la variable fictive ζ, se rappelant que A_1 est une constante dont la dérivée est nulle, il vient

$$\frac{dV_m}{d\zeta} = p_{m-1}\left[(m-1)A_1 p_m^{m-2} + (m-2)A_2 p_m^{m-3} + \ldots + 2A_{m-2}\,p_m + A_{m-1}\right]$$

$$+ \frac{dA_2}{d\zeta}p_m^{m-2} + \frac{dA_3}{d\zeta}p_m^{m-3} + \ldots + \frac{dA_{m-2}}{d\zeta}p_m^2 + \frac{dA_{m-1}}{d\zeta}p_m + \frac{dA_m}{d\zeta}.$$

Or, $\frac{dV_m}{d\zeta}$ est identiquement nul ; on a donc, en égalant à zéro les coefficients des puissances de p_m,

$$p_{m-1}A_{m-1} + \frac{dA_m}{d\zeta} = 0,$$

$$2p_{m-1}A_{m-2} + \frac{dA_{m-1}}{d\zeta} = 0,$$

$$3p_{m-1}A_{m-3} + \frac{dA_{m-2}}{d\zeta} = 0,$$

....

$$(m-3)p_{m-1}A_3 + \frac{dA_4}{d\zeta} = 0,$$

$$(m-2)p_{m-1}A_2 + \frac{dA_3}{d\zeta} = 0,$$

$$(m-1)p_{m-1}A_1 + \frac{dA_2}{d\zeta} = 0.$$

Or, si l'on connaît V_{m-1}, la valeur de A_m s'en déduit immédiatement, comme on l'a vu plus haut, et les équations précé-

dentes donneront ensuite successivement A_{m-1}, A_{m-2}, etc. En sorte que la valeur de V_m se déduit de celle de V_{m-1} par de simples différentiations.

EXEMPLE. — On a

$$V_2 = p_1^2 - 4p_2;$$

supposons qu'on veuille avoir V_3. On posera

$$V_3 = A_1 p_3^2 + A_2 p_3 + A_3,$$

et si l'on fait

$$\frac{dp_1}{d\zeta} = 3, \qquad \frac{dp_2}{d\zeta} = 2p_1,$$

on aura

$$p_3 A_2 + \frac{dA_3}{d\zeta} = 0, \qquad 2p_3 A_1 + \frac{dA_2}{d\zeta} = 0.$$

On a d'abord cette valeur de A_3, savoir,

$$A_3 = p_2^2 (p_1^2 - 4p_2) = p_1^2 p_2^2 - 4p_2^3,$$

on en déduit

$$\frac{dA_3}{d\zeta} = -18 p_1 p_2^2 + 4p_1^3 p_2,$$

et, par suite,

$$A_2 = 18 p_1 p_2 - 4p_1^3;$$

on trouve enfin,

$$\frac{dA_2}{d\zeta} = 54 p_2,$$

et, par suite,

$$A_1 = -27.$$

On a donc

$$V_3 = -27 p_3^2 + (18 p_1 p_2 - 4p_1^3) p_3 + p_1^2 p_2^2 - 4p_2^3.$$

Supposons encore qu'on veuille avoir V_4. On posera

$$V_4 = A_1 p_4^3 + A_2 p_4^2 + A_3 p_4 + A_4,$$

puis

$$\frac{dp_1}{d\zeta} = 4, \quad \frac{dp_2}{d\zeta} = 3p_1, \quad \frac{dp_3}{d\zeta} = 2p_2,$$

et

$$p_4 A_3 + \frac{dA_4}{d\zeta} = 0, \quad 2p_4 A_2 + \frac{dA_3}{d\zeta} = 0, \quad 3p_4 A_1 + \frac{dA_2}{d\zeta} = 0;$$

On a d'abord

$$A_4 = -27p_3^4 + 18\,p_1\,p_2\,p_3^3 - 4\,p_1^3\,p_3^3 + p_1^2\,p_2^2\,p_3^2 - 4\,p_2^3\,p_3^2,$$

d'où

$$\frac{dA_4}{d\zeta} = -144\,p_2\,p_3^3 + 6\,p_1^2\,p_3^3 + 80\,p_1\,p_2^2\,p_3^3 - 18\,p_1^3\,p_2\,p_3^2 + 4\,p_1^2\,p_2^3\,p_3 - 16\,p_2^4\,p_3,$$

et, par suite,

$$A_3 = 144\,p_2\,p_3^2 - 6\,p_1^3\,p_3^3 - 80\,p_1\,p_2^2\,p_3 + 18\,p_1^3\,p_2\,p_3 - 4\,p_1^2\,p_2^3 - 16\,p_2^4,$$

d'où

$$\frac{dA_3}{d\zeta} = 384\,p_1\,p_3^2 + 256\,p_2^2\,p_3 - 288\,p_1^3\,p_2\,p_3 + 54\,p_1^4\,p_3,$$

et, par suite,

$$A_3 = -192\,p_1\,p_3 - 128\,p_2^2 + 144\,p_1^2\,p_3 - 27\,p_1^4,$$

d'où

$$\frac{dA_2}{d\zeta} = -768\,p_3,$$

et, par suite,

$$A_1 = 256,$$

ce qui achève de déterminer la valeur de V_1.

Dans le cas particulier du quatrième degré, on peut mettre sous une forme commode pour le calcul arithmétique l'expression du produit des carrés des différences des racines. Prenons l'équation proposée sous la forme

$$ax^4 + 4\,bx^3 + 6\,cx^2 + 4\,dx + e = 0,$$

et soient

$$I = ae - 4\,bd + 3\,c^2,$$
$$J = ace + 2\,bcd - ad^2 - eb^2 - c^3.$$

On aura, en désignant les quatre racines par α, β, γ, δ,

$$a^6 \times (\alpha-\beta)^2(\alpha-\gamma)^2(\alpha-\delta)^2(\beta-\gamma)^2(\beta-\delta)^2(\gamma-\delta)^2 = 16\,(I^3 - 27\,J^2).$$

C'est M. Cayley qui, le premier, a trouvé cette formule.

NOTE IV.

SUR LA DÉCOMPOSITION DES FRACTIONS RATIONNELLES EN FRACTIONS SIMPLES.

Désignons par $F(x)$ une fonction rationnelle quelconque, par

$$x_1, \quad x_2, \ldots, \quad x_\mu$$

les racines de l'équation

$$\frac{1}{F(x)} = 0,$$

et par

$$m_1, \quad m_2, \ldots, \quad m_\mu$$

les degrés de multiplicité respectifs de ces racines.

Soit aussi, pour abréger,

$$\varphi(x) = (x - x_1)^{m_1} F(x),$$

$\varphi(x)$ désignant une fonction qui a une valeur finie différente de zéro pour $x = x_1$.

Si l'on imagine que la fonction rationnelle $F(x)$ soit décomposée en fractions simples, la somme des fractions relatives à la racine x_1 sera

$$\frac{\varphi(x_1)}{(x - x_1)^{m_1}} + \frac{\varphi'(x_1)}{1.(x - x_1)^{m_1 - 1}} + \ldots + \frac{\varphi^{m_1 - i - 1}(x_1)}{1.2\ldots(m_1 - i - 1)(x - x_1)^{i+1}} + \ldots + \frac{\varphi^{m_1 - 1}(x_1)}{1.2\ldots(m_1 - 1)(x - x_1)},$$

ainsi qu'on l'a vu dans la sixième leçon. Par suite, cette somme s'obtiendra en faisant $\zeta = 0$ dans l'expression

$$\frac{\varphi(x_1 + \zeta)}{(x - x_1 - \zeta)^{m_1}} + \frac{\varphi'(x_1 + \zeta)}{1.(x - x_1 - \zeta)^{m_1 - 1}} + \ldots + \frac{\varphi^{m_1 - i - 1}(x_1 + \zeta)}{1.2\ldots(m_1 - i - 1)(x - x_1 - \zeta)^{i+1}} + \ldots + \frac{\varphi^{m_1 - 1}(x_1 + \zeta)}{1.2\ldots(m_1 - 1)(x - x_1 - \zeta)}.$$

Or $\varphi'(x_1+\zeta)$, $\varphi''(x_1+\zeta)$, etc., peuvent être considérées comme les dérivées de $\varphi(x_1+\zeta)$ par rapport à la variable ζ, et alors il est aisé de voir que l'expression précédente se réduit à

$$\frac{1}{\Gamma(m_1)}\frac{d^{m_1-1}\dfrac{\varphi(x_1+\zeta)}{x-x_1-\zeta}}{d\zeta^{m_1-1}};$$

$\Gamma(\rho)$ désigne, comme dans les Notes précédentes, le produit des $\rho-1$ premiers nombres si ρ est plus grand que 1 et doit se réduire à l'unité pour $\rho=1$.

Comme on a

$$\varphi(x_1+\zeta)=\zeta^{m_1}F(x_1+\zeta),$$

la somme des fractions simples relatives à la racine x_1 sera égale à la valeur que prend, pour $\zeta=0$, l'expression suivante :

$$\frac{1}{\Gamma(m_1)}\frac{d^{m_1-1}\dfrac{\zeta^{m_1}F(x_1+\zeta)}{x-x_1-\zeta}}{d\zeta^{m_1-1}}.$$

Si donc la fonction rationnelle $F(x)$ ne contient pas de partie entière, on aura

$$F(x)=\sum\frac{1}{\Gamma(m_1)}\frac{d^{m_1-1}\dfrac{\zeta^{m_1}F(x_1+\zeta)}{x-x_1-\zeta}}{d\zeta^{m_1-1}}.$$

Dans cette formule, il faut faire $\zeta=0$, après les différentiations; le signe sommatoire $\sum$ s'étend à toutes les racines $x_1, x_2,\ldots, x_\mu$. Il est presque superflu d'ajouter que si le degré de multiplicité d'une racine, de x_1 par exemple, se réduit à 1, la dérivée

$$\frac{d^{m_1-1}\dfrac{\zeta^{m_1}F(x_1+\zeta)}{x-x_1-\zeta}}{d\zeta^{m_1-1}} \text{ se réduit à } \frac{\zeta F(x_1+\zeta)}{x-x_1-\zeta}.$$

On obtient, d'après cela, cette expression très-simple de l'in-

tégrale $\int F(x)\,dx$, savoir:

$$\int F(x)\,dx = \sum \frac{1}{\Gamma(m_1)} \frac{d^{m_1-1} \zeta^{m_1} F(x_1+\zeta)\log(x-x_1-\zeta)}{d\zeta^{m_1-1}}.$$

Si la fonction $F(x)$ contient une partie entière $E(x)$, on a

$$F(x) = E(x) + \sum \frac{1}{\Gamma(m_1)} \frac{d^{m_1-1} \dfrac{\zeta^{m_1} F(x_1+\zeta)}{x-x_1-\zeta}}{d\zeta^{m_1-1}};$$

il est aisé de trouver la valeur de $E(x)$. Désignons par n l'excès du degré du numérateur de $F(x)$ sur celui du dénominateur; n sera le degré de $E(x)$. Cela posé, si l'on change x en $\frac{1}{z}$ dans l'équation précédente et qu'on multiplie ensuite, de part et d'autre, par z^n, on aura

$$z^n F\left(\frac{1}{z}\right) = z^n E\left(\frac{1}{z}\right) + z^{n+1} \sum \frac{1}{\Gamma(m_1)} \frac{d^{m_1-1} \dfrac{\zeta^{m_1} F(x_1+\zeta)}{1-(x_1+\zeta)z}}{d\zeta^{m_1-1}}.$$

Il s'ensuit que si l'on développe $z^n F\left(\frac{1}{z}\right)$ en série ordonnée, suivant les puissances croissantes de z, la somme des termes dont le degré ne surpasse pas n sera $z^n E\left(\frac{1}{z}\right)$. Or, ζ désignant toujours un infiniment petit, on a, par la formule de Maclaurin,

$$z^n F\left(\frac{1}{z}\right) = \zeta^n F\left(\frac{1}{\zeta}\right) + \frac{z}{1} \frac{d\zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta} + \frac{z^2}{1.2} \frac{d^2 \zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta^2} + \ldots;$$

donc on a

$$z^n E\left(\frac{1}{z}\right) = \zeta^n F\left(\frac{1}{\zeta}\right) + \frac{z}{1} \frac{d\zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta} + \ldots + \frac{z^n}{1.2\ldots n} \frac{d^n \zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta^n},$$

et, par suite,

$$E(x) = x^n \zeta^n F\left(\frac{1}{\zeta}\right) + x^{n-1} \frac{d\zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta}$$

$$+ \frac{x^{n-2}}{1.2} \frac{d^2 \zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta^2} + \ldots + \frac{1}{1.2\ldots n} \frac{d^n \zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta^n}.$$

On peut trouver une autre expression plus simple du polynôme $E(x)$. En effet, le coefficient de ζ^{n-i} dans le développement de $\zeta^n F\left(\frac{1}{\zeta}\right)$, suivant les puissances croissantes de ζ, est égal au coefficient de ζ^n dans le développement de $\zeta^{n+i} F\left(\frac{1}{\zeta}\right)$; d'ailleurs, ces coefficients sont les valeurs que prennent, pour $\zeta = 0$, les deux quantités

$$\frac{1}{\Gamma(n-i+1)} \frac{d^{n-i} \zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta^{n-i}}, \quad \frac{1}{\Gamma(n+1)} \frac{d^n \zeta^{n+i} F\left(\frac{1}{\zeta}\right)}{d\zeta^n};$$

donc on a, pour $\zeta = 0$,

$$\frac{1}{\Gamma(n-i+1)} \frac{d^{n-i} \zeta^n F\left(\frac{1}{\zeta}\right)}{d\zeta^{n-i}} = \frac{1}{\Gamma(n+1)} \frac{d^n \zeta^{n+i} F\left(\frac{1}{\zeta}\right)}{d\zeta^n};$$

et il faut remarquer que le premier membre doit être réduit à $\zeta^n F\left(\frac{1}{\zeta}\right)$ dans le cas de $i = n$.

D'après cela, la valeur de $E(x)$ devient

$$E(x) = \frac{1}{\Gamma(n+1)} \frac{d^n \zeta^n F\left(\frac{1}{\zeta}\right)(1 + \zeta x + \zeta^2 x^2 + \ldots + \zeta^n x^n)}{d\zeta^n};$$

enfin, comme on a évidemment, pour $\zeta = 0$, et pour $i > n$,

$$\frac{d^n \zeta^{n+i} F\left(\frac{1}{\zeta}\right)}{d\zeta^n} = 0,$$

on peut aussi écrire

$$E(x) = \frac{1}{\Gamma(n+1)} \frac{d^n \zeta^n F\left(\frac{1}{\zeta}\right)(1+\zeta x+\zeta^2 x^2+\ldots+\zeta^n x^n+\zeta^{n+1} x^{n+1}+\ldots)}{d\zeta^n},$$

ou

$$E(x) = \frac{1}{\Gamma(n+1)} \frac{d^n \dfrac{\zeta^n F\left(\frac{1}{\zeta}\right)}{1-\zeta x}}{d\zeta^n}.$$

On a donc la formule suivante qui donne la valeur d'une fonction rationnelle quelconque $F(x)$ décomposée en une partie entière et en fractions simples, savoir :

$$F(x) = \frac{1}{\Gamma(n+1)} \frac{d^n \dfrac{\zeta^n F\left(\frac{1}{\zeta}\right)}{1-\zeta x}}{d\zeta^n} + \sum \frac{1}{\Gamma(m_1)} \frac{d^{m_1-1} \dfrac{\zeta^{m_1} F(x_1+\zeta)}{x-x_1-\zeta}}{d\zeta^{m_1-1}},$$

la quantité ζ devant être égalée à zéro après les différentiations.

NOTE V.

SUR UNE APPLICATION DE LA MÉTHODE DE TSCHIRNAUS.

M. Jerrard, géomètre anglais, a démontré, dans ces derniers temps, qu'on peut faire disparaître d'une équation quelconque le deuxième, le troisième et le quatrième terme par la résolution d'une seule équation du troisième degré. Nous allons démontrer ici ce remarquable théorème.

Nous commencerons par établir le lemme suivant :

Une fonction homogène et entière du second degré de n quantités est la somme des carrés de n fonctions linéaires.

Soit V une fonction homogène et entière du second degré des n quantités

$$a_0,\ a_1,\ a_2, \ldots,\ a_{n-1};$$

en l'ordonnant par rapport à a_{n-1}, on aura

$$V = Pa_{n-1}^2 + Qa_{n-1} + R;$$

P est une constante, Q une fonction homogène et linéaire des $n-1$ quantités $a_0,\ a_1, \ldots, a_{n-2}$, enfin R est une fonction homogène et du second degré de ces mêmes quantités. On peut écrire aussi

$$V = \left(a_{n-1}\sqrt{P} + \frac{Q}{2\sqrt{P}}\right)^2 + R - \frac{Q^2}{4P},$$

ce qui montre que V est égal au carré d'une fonction linéaire des n quantités $a_0,\ a_1, \ldots, a_{n-1}$, augmentée d'une fonction entière et homogène du second degré des $n-1$ quantités $a_0,\ a_1, \ldots, a_{n-2}$. En opérant sur cette dernière, comme on a fait sur V, on la décomposera en deux parties dont l'une sera le carré d'une fonction linéaire de $n-1$ quantités et dont l'autre sera une fonction entière et homogène du second degré de $n-2$ quantités seulement. Et, en continuant ainsi, on mettra V sous la forme suivante :

$$V = V_1^2 + V_2^2 + V_3^2 + \ldots + V_{n-1}^2 + V_n^2,$$

V_1, V_2, $V_3, \ldots$, V_n étant des fonctions linéaires qui renferment respectivement n, $n-1$, $n-2, \ldots$, 1 quantités; ce qui démontre la proposition énoncée.

Passons maintenant à la démonstration du théorème que nous avons en vue. Soit l'équation

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} + \ldots + p_{m-1} x + p_m = 0,$$

et posons

$$y = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4.$$

Soit aussi

$$y^m + q_1 y^{m-1} + q_2 y^{m-2} + q_3 y^{m-3} + \ldots + q_{m-1} y + q_m = 0$$

l'équation en y. D'après ce qu'on a vu dans la huitième leçon, la somme des puissances $\rho^{\text{ièmes}}$ des racines de l'équation en y est une fonction homogène et entière du degré ρ des cinq quantités a_0, a_1, a_2, a_3, a_4; par suite, les coefficients $q_1, q_2, \ldots, q_m$ sont aussi des fonctions entières et homogènes des mêmes quantités, et les degrés de ces fonctions q sont précisément égaux à leurs indices. Cela posé, pour faire disparaître le second, le troisième et le quatrième terme de l'équation en y, il faut faire

$$q_1 = 0, \quad q_2 = 0, \quad q_3 = 0.$$

La première de ces équations est linéaire; tirons-en la valeur de a_0 en fonction de a_1, a_2, a_3, a_4 pour la porter dans les deux autres, et supposons que celles-ci deviennent

$$q'_2 = 0, \quad q'_3 = 0.$$

Les premiers membres de ces équations sont des fonctions homogènes des degrés 2 et 3 respectivement des quatre quantités a_1, a_2, a_3, a_4. Or, d'après le lemme qui a été démontré en commençant, l'équation $q'_2 = 0$ peut se mettre sous la forme

$$f^2 + g^2 + h^2 + k^2 = 0,$$

f, g, h, k étant des fonctions linéaires, et cette équation sera satisfaite en posant

$$f^2 + g^2 = 0, \quad h^2 + k^2 = 0,$$

ou

$$f = g\sqrt{-1}, \quad h = k\sqrt{-1}.$$

Ces deux dernières équations sont linéaires; si l'on en tire les valeurs de a_1 et a_2 pour les porter dans l'équation $q'_3=0$, celle-ci deviendra

$$q''_3 = 0,$$

et son premier membre q''_3 sera une fonction homogène et du troisième degré des deux quantités a_3 et a_4. L'une de ces quantités peut être prise arbitrairement, et l'autre dépend, comme on voit, d'une équation du troisième degré. Les quantités a_3 et a_4 étant déterminées, les valeurs de a_0, a_1, a_2 le seront aussi immédiatement. L'équation en y se réduit alors à

$$y^m + q_4 y^{m-4} + \ldots + q_{m-1} y + q_m = 0.$$

Par la même transformation on peut faire disparaître le deuxième, le troisième et le cinquième terme d'une équation quelconque; seulement, la détermination des arbitraires a_0, a_1, a_2, a_3, a_4 exige la résolution d'une équation du quatrième degré au lieu de celle d'une équation du troisième degré.

Enfin, si à la transformation de Tschirnaüs on joint la transformation qui consiste à remplacer l'inconnue par son inverse, on voit que, par le moyen d'une seule équation du troisième ou du quatrième degré, il est possible de faire disparaître d'une équation quelconque les trois termes qui précèdent le dernier ou bien les deux qui précèdent le dernier avec celui qui précède le dernier de quatre rangs. Et, dans le cas particulier de l'équation du cinquième degré, il est clair qu'on peut faire disparaître ainsi trois termes quelconques entre le premier et le dernier. Ainsi, par la transformation dont il s'agit, l'équation du cinquième degré peut toujours être ramenée à l'une quelconque des quatre formes

$$x^5 + px + q = 0,$$
$$x^5 + px^2 + q = 0,$$
$$x^5 + px^3 + q = 0,$$
$$x^5 + px^4 + q = 0.$$

NOTE VI.

SUR L'ÉLIMINATION D'UNE INCONNUE ENTRE DEUX ÉQUATIONS.

Nous avons fait connaître, dans la troisième leçon, la méthode fondée sur la théorie des fonctions symétriques, pour former l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations; nous avons démontré ensuite que le degré de l'équation finale relative à deux équations générales des degrés m et n respectivement est précisément égal à mn, et que, dans aucun cas, ce degré ne peut surpasser le produit des degrés des équations proposées. Nous sommes revenu sur cette question dans la neuvième leçon; mais, à l'égard des équations particulières, nous nous sommes borné encore, comme nous l'avions fait précédemment, à assigner la limite que ne peut dépasser le degré de l'équation finale. Nous allons indiquer dans cette Note, d'après M. Minding, un moyen simple de déterminer avec précision le degré de l'équation finale relative à deux équations quelconques données (*).

Développement d'une fonction algébrique implicite en série ordonnée suivant les puissances décroissantes de sa variable.

Soit

$$(1) \qquad M(x, y) = 0$$

une équation entre les deux variables x et y. Les racines y sont des fonctions de x, et si l'équation est complète, chaque racine,

(*) Une traduction du Mémoire de M. Minding a été publiée dans le tome VI du *Journal de Mathématiques pures et appliquées*. La méthode employée par ce géomètre repose sur des considérations analogues à celles que nous avons développées dans la neuvième leçon.

ainsi qu'on l'a vu dans la neuvième leçon, peut être développée dans une série de la forme

$$y = \alpha x + \alpha' + \frac{\alpha''}{x} + \frac{\alpha'''}{x^2} + \ldots.$$

En sorte que, dans le cas général, les racines y d'une équation à deux variables x et y sont du premier degré par rapport à x (*). Mais il n'en est pas toujours ainsi, lorsque l'équation que l'on considère manque de quelques termes. Nous allons indiquer un procédé pour trouver généralement les degrés des racines y de l'équation (1), et pour former les développements de ces racines en séries ordonnées suivant les puissances décroissantes de x.

En ordonnant l'équation (1) par rapport aux puissances décroissantes de y, nous l'écrirons de la manière suivante :

$$(2)\quad \mathrm{A}y^{m} + \mathrm{A}_1 y^{m_1} + \ldots + \mathrm{A}_k y^{m_k} + \ldots + \mathrm{A}_i y^{m_i} + \mathrm{A}_{i+1} = 0,$$

et nous désignerons par

$$\mu, \quad \mu_1, \quad \mu_2, \ldots, \quad \mu_k, \ldots, \quad \mu_i, \quad \mu_{i+1}$$

les degrés des coefficients

$$\mathrm{A}, \quad \mathrm{A}_1, \quad \mathrm{A}_2, \ldots, \quad \mathrm{A}_k, \ldots, \quad \mathrm{A}_i, \quad \mathrm{A}_{i+1},$$

qui sont des fonctions entières de x.

Cela posé, désignons par r un exposant indéterminé, par u une nouvelle variable, et faisons

$$y = ux^r;$$

l'équation (2) devient

$$(3)\quad \mathrm{A}x^{mr}u^{m} + \mathrm{A}_1 x^{m_1 r}u^{m_1} + \ldots + \mathrm{A}_k x^{m_k r}u^{m_k} + \ldots + \mathrm{A}_{i+1} = 0,$$

(*) On dit qu'une fonction y de x est du degré r lorsque le quotient $\frac{y}{x^r}$ n'est ni nul ni infini pour $x = \infty$.

ou, en divisant par $A x^{mr}$,

$$(4)\quad u^m + \frac{A_1 x^{-(m-m_1)r}}{A} u^{m_1} + \ldots + \frac{A_k x^{-(m-m_k)r}}{A} u^{m_k} + \ldots + \frac{A_{i+1} x^{-mr}}{A} = 0\,;$$

dans cette équation, les degrés relatifs à x des coefficients des termes qui suivent le premier sont respectivement

$$(5)\quad \left\{ \begin{array}{l} (m - m_1)\left(\dfrac{\mu_1 - \mu}{m - m_1} - r\right), \ldots, \\ (m - m_k)\left(\dfrac{\mu_k - \mu}{m - m_k} - r\right), \ldots, \quad m\left(\dfrac{\mu_{i+1} - \mu}{m} - r\right). \end{array} \right.$$

Désignons par ρ_1 le plus grand des nombres

$$\frac{\mu_1 - \mu}{m - m_1}, \ldots, \quad \frac{\mu_k - \mu}{m - m_k}, \ldots, \quad \frac{\mu_i - \mu}{m - m_i}, \quad \frac{\mu_{i+1} - \mu}{m},$$

et supposons que $\dfrac{\mu_k - \mu}{m - m_k}$ soit le dernier de ceux qui sont égaux à ρ_1. Si l'on fait $r = \rho_1$, quelques-uns des nombres (5) seront nuls, mais tous les autres, et en particulier ceux qui suivent le $k^{\text{ième}}$, seront négatifs; en sorte que, pour $x = \infty$, l'équation (4) prendra la forme

$$u^m + \ldots + B_k u^{m_k} = 0, \quad \text{ou} \quad u^{m_k} f(u) = 0,$$

les coefficients B ayant des valeurs finies et le dernier d'entre eux B_k étant différent de zéro. Cette équation (6) a m_k racines nulles, et $m - m_k$ racines finies et différentes de zéro. Il s'ensuit que, parmi les racines y de l'équation (2), il y en a m_k dont les degrés sont inférieurs à ρ_1, et $m - m_k$ dont les degrés sont égaux à ρ_1. En outre, les premiers termes des séries qui représentent ces dernières racines sont égaux aux diverses valeurs de αx^{ρ_1} quand on prend successivement pour α, chacune des racines de l'équation

$$f(\alpha) = 0.$$

Cherchons maintenant les premiers termes des séries qui re-

présentent les m_k racines y de degré inférieur à ρ_1. En divisant l'équation (3) par $A_k x^{m_k r}$, elle devient

$$(7)\quad \left\{\begin{aligned} &\frac{A x^{(m-m_k)r}}{A_k} u^m + \ldots + u^{m_k} + \ldots \\ &+ \frac{A_{k'} x^{(m_{k'}-m_k)r}}{A_k} u^{m_{k'}} + \ldots + \frac{A_{i+1} x^{-m_k r}}{A_k} = 0; \end{aligned}\right.$$

les coefficients des termes qui précèdent u^{m_k} ont pour degrés

$$(8)\quad -(m - m_k)\left(\frac{\mu_k - \mu}{m - m_k} - r\right), \ldots, \quad -(m_{k-1} - m_k)\left(\frac{\mu_k - \mu_{k-1}}{m_{k-1} - m_k} - r\right),$$

et ceux des termes qui suivent u^{m_k} ont pour degrés

$$(9)\quad \left\{\begin{aligned} &(m_k - m_{k+1})\left(\frac{\mu_{k+1} - \mu_k}{m_k - m_{k+1}} - r\right), \ldots, \\ &(m_k - m_{k'})\left(\frac{\mu_{k'} - \mu_k}{m_k - m_{k'}} - r\right), \ldots, \quad m_k\left(\frac{\mu_{i+1} - \mu_k}{m_k} - r\right). \end{aligned}\right.$$

Désignons par ρ_2 le plus grand des nombres

$$\frac{\mu_{k+1} - \mu_k}{m_k - m_{k+1}}, \ldots, \quad \frac{\mu_{k'} - \mu_k}{m_k - m_{k'}}, \ldots, \quad \frac{\mu_{i+1} - \mu_k}{m_k},$$

et supposons que $\dfrac{\mu_{k'} - \mu_k}{m_k - m_{k'}}$ soit le dernier de ceux qui sont égaux à ρ_2. Il est aisé de voir que ρ_2 est plus petit que ρ_1. En effet, on a, par hypothèse,

$$\frac{\mu_k - \mu}{m - m_k} = \rho_1 \quad \text{et} \quad \frac{\mu_{k'} - \mu}{m - m_{k'}} < \rho_1,$$

et l'on en déduit

$$\frac{\mu_{k'} - \mu_k}{m_k - m_{k'}} < \rho_1, \quad \text{ou} \quad \rho_2 < \rho_1.$$

Si l'on fait $r = \rho_2$, les nombres (9) sont nuls ou négatifs, et en particulier tous ceux qui suivent le $(k' - k)^{\text{ième}}$ sont négatifs. On

voit aussi que tous les nombres (8) sont négatifs; car si g est $< k$, on a, par hypothèse,

$$\frac{\mu_g - \mu}{m - m_g} = \text{ ou } < \rho_1 \quad \text{avec} \quad \frac{\mu_k - \mu}{m - m_k} = \rho_1,$$

d'où

$$\frac{\mu_k - \mu_g}{m_g - m_k} = \text{ ou } > \rho_1 \quad \text{et} \quad \frac{\mu_k - \mu_g}{m_g - m_k} - \rho_2 > 0.$$

D'après cela, si l'on y fait $r = \rho_2$ et $x = \infty$, l'équation (7) prendra la forme

$$(10) \qquad u^{m_k} + \ldots + B_{k'} u^{m_{k'}} = 0, \quad \text{ou} \quad u^{m_{k'}} f_1(u) = 0,$$

les coefficients B ayant des valeurs finies et le dernier $B_{k'}$ étant différent de zéro. Cette équation (10) a $m_{k'}$ racines nulles et $m_k - m_{k'}$ racines finies et différentes de zéro. Il s'ensuit que, parmi les racines y de l'équation (2), il y en a $m_{k'}$ dont les degrés sont inférieurs à ρ_2, et $m_k - m_{k'}$ dont les degrés sont égaux à ρ_2. En outre, les premiers termes des séries qui représentent ces dernières racines seront égaux aux valeurs de αx^{ρ_2} quand on prend successivement pour α chacune des racines de l'équation

$$f_1(\alpha) = 0.$$

En continuant de la même manière, on déterminera les premiers termes des séries qui représentent les $m_{k'}$ racines de degré inférieur à ρ_2. Ce que nous avons dit suffit évidemment pour établir le théorème suivant :

Étant donnée l'équation

$$Ay^m + A_1 y^{m_1} + \ldots + A_i y^{m_i} + A_{i+1} = 0,$$

ordonnée par rapport aux puissances décroissantes de y, et dans laquelle les coefficients

$$A, \; A_1, \; A_2, \ldots, \; A_{i+1}$$

sont des fonctions entières de x ayant respectivement pour degrés

$$\mu, \; \mu_1, \; \mu_2, \ldots, \; \mu_{i+1},$$

si ρ_1 désigne le plus grand des nombres

$$\frac{\mu_1-\mu}{m-m_1},\quad \frac{\mu_2-\mu}{m-m_2},\ldots,\quad \frac{\mu_{i+1}-\mu}{m},$$

et que $\frac{\mu_k-\mu}{m-m_k}$ *soit le dernier de ceux dont la valeur est* ρ_1, *l'équation proposée aura* $m-m_k$ *racines de degré* ρ_1, *et si k est* $< i+1$, *les* m_k *autres racines seront de degré inférieur à* ρ_1. *Si, en second lieu,* ρ_2 *désigne le plus grand des nombres*

$$\frac{\mu_{k+1}-\mu_k}{m_k-m_{k+1}},\quad \frac{\mu_{k+2}-\mu_k}{m_k-m_{k+2}},\ldots,\quad \frac{\mu_{i+1}-\mu_k}{m_k},$$

et que $\frac{\mu_{k'}-\mu_k}{m_k-m_{k'}}$ *soit le dernier de ceux dont la valeur est* ρ_2, *l'équation proposée aura* $m_k-m_{k'}$ *racines de degré* ρ_2, *et si* k' *est* $< i+1$, *les* $m_{k'}$ *autres racines seront de degré inférieur à* ρ_2. *Si, en troisième lieu,* ρ_3 *désigne le plus grand des nombres*

$$\frac{\mu_{k'+1}-\mu_{k'}}{m_{k'}-m_{k'+1}},\quad \frac{\mu_{k'+2}-\mu_{k'}}{m_{k'}-m_{k'+2}},\ldots,\quad \frac{\mu_{i+1}-\mu_{k'}}{m_{k'}},$$

et que $\frac{\mu_{k''}-\mu_{k'}}{m_{k'}-m_{k''}}$ *soit le dernier de ceux dont la valeur est* ρ_3, *l'équation proposée aura* $m_{k'}-m_{k''}$ *racines de degré* ρ_3, *et si* k'' *est* $< i+1$, *les* $m_{k''}$ *autres racines seront de degré inférieur à* ρ_3. *Et ainsi de suite*

Quand on aura trouvé les premiers termes des series qui représentent les diverses racines y de l'équation proposée, on obtiendra aisément et de la même manière autant de termes qu'on voudra de ces séries. Considérons, par exemple, une racine dont le premier terme soit αx^{ρ}, on posera

$$y=\alpha x^{\rho}+z;$$

si la proposée n'a qu'une seule racine dont le premier terme soit αx^{ρ}, la transformée en z n'aura qu'une seule racine de degré inférieur à ρ, et si la proposée a plusieurs racines

ayant αx^{ρ} pour premier terme, la transformée aura un pareil nombre de racines de degré inférieur à ρ. On trouvera les premiers termes de ces racines de l'équation en z, comme on a trouvé les premiers termes des racines de l'équation en y ; on connaîtra ainsi les deux premiers termes des racines de l'équation en y qui ont αx^{ρ} pour premier terme. Et, en suivant la même marche, on calculera autant de termes que l'on voudra des racines de l'équation en y.

Exemple. — Proposons-nous de trouver les degrés des racines y de l'équation

$$(x,8)y^5+(x,6)y^4+(x,9)y^3+(x,4)y^2+(x,3)y+(x,4)=0\,;$$

nous désignons, avec Bezout, par la notation (x, μ) un polynôme en x du degré μ.

D'après le théorème que nous avons établi plus haut, il faut d'abord former les nombres

$$-2,\quad \frac{1}{2},\quad -\frac{4}{3},\quad -\frac{5}{4},\quad -\frac{4}{5},$$

dont le maximum est $\frac{1}{2}$; le dernier nombre égal à ce maximum occupant le deuxième rang, l'équation proposée a deux racines de degré $\frac{1}{2}$. Pour avoir les degrés des autres racines, il faut former les nombres

$$-5,\quad -3,\quad -\frac{5}{3},$$

dont le maximum est $-\frac{5}{3}$; le seul nombre égal à ce maximum occupant le troisième rang, l'équation proposée a trois racines du degré $-\frac{5}{3}$.

Formation de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations quelconques à deux inconnues. — Détermination du degré de l'équation finale.

Soient les deux équations

$$(1)\quad M(x,y) = Ay^m + A_1 y^{m-1} + \ldots + A_i y^{m-i} + A_{i+1} = 0,$$

$$(2)\quad N(x,y) = By^n + B_1 y^{n-1} + \ldots + B_j y^{n-j} + B_{j+1} = 0,$$

que nous supposons ordonnées par rapport aux puissances décroissantes de y, et dans lesquelles les coefficients A, $A_1, \ldots$, B, $B_1, \ldots$ sont des fonctions entières de x. Il s'agit de former l'équation finale qui résulte de l'élimination de y.

Désignons par $y_1, y_2, \ldots, y_m$ les racines de l'équation (1) résolue par rapport à y, par $n_1, n_2, \ldots, n_n$, les racines de l'équation (2), et posons

$$P = M(x, n_1)\, M(x, n_2) \ldots M(x, n_n),$$
$$Q = N(x, y_1)\, N(x, y_2) \ldots N(x, y_m).$$

On a

$$M(x, y) = A(y - y_1)(y - y_2) \ldots (y - y_m),$$
$$N(x, y) = B(y - n_1)(y - n_2) \ldots (y - n_n);$$

d'où

$$M(x, n_1) = A(n_1 - y_1)(n_1 - y_2) \ldots (n_1 - y_m),$$
$$M(x, n_2) = A(n_2 - y_1)(n_2 - y_2) \ldots (n_2 - y_m),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$M(x, n_n) = A(n_n - y_1)(n_n - y_2) \ldots (n_n - y_m).$$

Il suit de là que $\frac{P}{A^n}$ est égal au produit des différences qu'on obtient en retranchant chacune des racines $y_1, y_2, \ldots, y_m$ de chacune des racines $n_1, n_2, \ldots, n_n$. On trouverait de même que $\frac{Q}{B^m}$ est égal au produit des différences qu'on obtient en retranchant chaque racine n de chaque racine y, et comme le

nombre de ces différences est mn, on a

$$\frac{P}{A^n} = (-1)^{mn} \frac{Q}{B^m},$$

ou

(3) $$B^m P = (-1)^{mn} A^n Q.$$

Or, P est une fonction entière et symétrique des racines de l'équation (2), et ses coefficients sont des fonctions entières des coefficients de l'équation (1); donc $B^m P$ est une fonction rationnelle des coefficients des équations proposées et qui même est entière par rapport aux coefficients de l'équation (1). Pour la même raison, $A^n Q$ est une fonction rationnelle des coefficients des équations proposées et qui est entière par rapport aux coefficients de l'équation (2). Donc, à cause de l'équation (3), $B^m P$ est une fonction entière des coefficients des équations (1) et (2), et, par suite, elle est une fonction entière de x. Nous la désignerons par $F(x)$, et nous allons montrer que

(4) $$F(x) = 0$$

est l'équation finale qui résulte de l'élimination de y entre les équations proposées. En effet, soit a une valeur de x, répondant à la question; c'est-à-dire telle, que les équations

$$M(a, y) = 0, \quad N(a, y) = 0,$$

aient au moins une racine commune; on a nécessairement, pour $x = a$, $P = 0$ et $Q = 0$, et, par suite, $F(x) = 0$. Réciproquement, soit a une racine de $F(x) = 0$; à cause de

$$B^m P = (-1)^{mn} A^n Q = F(x),$$

on a nécessairement $P = 0$ et $Q = 0$ pour $x = a$, et, par suite, les équations

$$M(a, y) = 0, \quad N(a, y) = 0$$

ont au moins une racine commune. Ceci suppose toutefois que A et B ne soient pas nuls en même temps, pour $x = a$; mais il est évident que les équations proposées admettent alors la solution commune $x = a, y = \infty$. Au surplus, on peut exclure

ce cas particulier en changeant infiniment peu les coefficients des polynômes A et B sans changer leurs degrés; d'où il suit que l'équation (4) n'aura jamais de racine étrangère. Et cette considération permet aussi de voir que si A et B ont un facteur commun, le polynôme $F(x)$ sera divisible par ce facteur.

Lorsque les polynômes A, $A_1,\ldots$, B, $B_1,\ldots$, sont chacun le plus général possible de son degré, les équations (1) et (2) n'ont pas de solutions multiples et ne peuvent acquérir qu'une seule racine commune y pour chaque racine de l'équation finale. Mais le contraire peut arriver si les coefficients des polynômes A, $A_1,\ldots$, B, $B_1,\ldots$, ont des valeurs déterminées. Dans ce cas, chaque racine de l'équation finale a le degré de multiplicité convenable; il suffit, pour s'en convaincre, de changer infiniment peu les coefficients des polynômes A, $A_1,\ldots$, B, $B_1,\ldots$, et de supposer ensuite ces changements nuls.

Passons maintenant à la détermination du degré de l'équation finale. Pour cela, on cherchera les degrés $\rho_1, \rho_2,\ldots, \rho_n$ des racines $n_1, n_2,\ldots, n_n$ de l'équation (2), et l'on en conclura aisément les degrés $\lambda_1, \lambda_2,\ldots, \lambda_n$ des fonctions $M(x, n_1)$, $M(x, n_2),\ldots, M(x, n_n)$. Ces degrés λ peuvent être fractionnaires, mais ne sont jamais négatifs, parce que le polynôme A_{i+1} est au moins du degré zéro. Enfin, si l'on désigne par ν le degré du polynôme B, il est évident que le degré de $B^m P$ ou $F(x)$ sera

$$m\nu + \lambda_1 + \lambda_2 + \ldots + \lambda_n.$$

Il peut arriver, dans quelques cas particuliers, qu'il ne suffise pas de déterminer les degrés $\rho_1, \rho_2,\ldots, \rho_n$ pour connaître $\lambda_1, \lambda_2,\ldots, \lambda_n$, et qu'il soit nécessaire de calculer entièrement un ou plusieurs termes des séries qui représentent les racines $n_1, n_2,\ldots, n_n$. Mais il est évident que ces cas particuliers ne peuvent se présenter que si la série dans laquelle se développe l'une des racines $n_1, n_2,\ldots, n_n$, coïncide, dans quelques-uns de ses premiers termes, avec la série dans laquelle se développe l'une des racines $y_1, y_2,\ldots, y_m$.

Soient, pour exemple, les deux équations

$$(x, 2)y^4 + (x, 2)y^3 + (x, 4)y^2 + (x, 5)y + (x, 5) = 0,$$
$$(x, 8)y^5 + (x, 6)y^4 + (x, 9)y^3 + (x, 4)y^2 + (x, 3)y + (x, 4) = 0,$$

où (x, μ) désigne, comme plus haut, un polynôme quelconque du degré μ.

Les degrés $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ des racines de la seconde équation ont ici pour valeurs

$$\rho_1 = \rho_2 = \frac{1}{2}, \qquad \rho_3 = \rho_4 = \rho_5 = -\frac{5}{3};$$

on en déduit

$$\lambda_1 = \lambda_2 = \frac{11}{2}, \qquad \lambda_3 = \lambda_4 = \lambda_5 = 5.$$

D'ailleurs, $\nu = 8$ et $m = 4$, donc le degré de l'équation finale est ici

$$4.8 + 11 + 15 = 58;$$

la limite assignée par le théorème de Bezout est 6.13 ou 78.

Lorsqu'on a deux équations entre deux inconnues x et y, il peut arriver que l'équation finale résultant de l'élimination de y ne soit pas du même degré que l'équation résultant de l'élimination de x. Il est aisé d'expliquer la raison de ce fait : l'équation finale en x donne seulement les valeurs finies de x propres à satisfaire aux deux équations proposées; si donc l'équation finale en y est d'un degré plus élevé que celle en x, il y a nécessairement quelques racines de l'équation en y qui correspondent à des valeurs infinies de x. Nous avons suffisamment indiqué plus haut le moyen de découvrir ces valeurs.

NOTE VII.

SUR UNE CLASSE D'ÉQUATIONS QUI POSSÈDENT UNE PROPRIÉTÉ REMARQUABLE.

Dans un Mémoire publié au tome IX du Journal de M. Liouville, M. Lobatto a fait connaître la forme générale des équations du troisième degré *dépourvues du second terme* qui possèdent une propriété remarquable observée depuis longtemps (*). Cette propriété des équations dont je parle consiste en ce que, si l'on développe leurs racines en fraction continue, d'après la méthode de Lagrange, les trois fractions continues que l'on obtient sont terminées par les mêmes quotients.

J'ai reproduit, dans la seizième leçon, l'analyse de M. Lobatto, en y apportant toutefois quelques modifications, et j'ai indiqué aussi comment on pourrait former les équations complètes du troisième degré qui ont cette même propriété.

Je me propose, dans cette Note, de résoudre le problème plus général dont voici l'énoncé (**) :

Quelles sont les équations irréductibles jouissant de la propriété que, si l'on développe leurs racines réelles en fraction continue par la méthode de Lagrange, deux ou plusieurs de ces fractions continues soient terminées par les mêmes quotients ?

On verra que les équations irréductibles dont il s'agit ont un degré de la forme $2n$ ou de la forme $3n$. On peut partager leurs racines en n groupes composés chacun de deux ou trois racines, suivant que le degré est $2n$ ou $3n$; si les racines d'un même

(*) M. Vincent, dans son remarquable Mémoire *Sur la résolution des équations numériques*, l'a observée sur l'équation $x^3 - 7x + 7 = 0$ (tome Ier du Journal de M. Liouville), et il ajoute : « Cette propriété mériterait peut-être un examen spécial. »

(**) Cette Note est la reproduction d'un Mémoire que j'ai publié dans le tome XV du Journal de M. Liouville.

groupe sont réelles, les fractions continues qui les représentent sont terminées par les mêmes quotients.

Je donnerai, en même temps, la forme générale des équations qui possèdent cette singulière propriété.

Condition pour que les fractions continues qui représentent deux irrationnelles soient terminées par les mêmes quotients.

Si deux irrationnelles x et x' sont telles, que les fractions continues dans lesquelles elles se développent aient un même quotient complet y, on aura, par les propriétés des fractions continues,

$$(1) \qquad x = \frac{qy+p}{q'y+p'}, \qquad x' = \frac{sy+r}{s'y+r'},$$

p, q, p', etc., étant des entiers qui satisfont aux deux conditions

$$(2) \qquad qp' - pq' = \pm 1, \quad sr' - rs' = \pm 1;$$

en outre, on peut supposer p', q', r', s' positifs, q et p seront de même signe que x, r et s de même signe que x'. Des équations (1) on tire

$$x' = \frac{ax+b}{a'x+b'},$$

en posant

$$a = rq' - sp', \qquad b = sp - rq,$$
$$a' = r'q' - s'p', \quad b' = s'p - r'q,$$

équations dont on déduit

$$ab' - ba' = (qp' - pq')(sr' - rs') = \pm 1.$$

Donc, pour que deux irrationnelles positives ou négatives x et x' puissent se développer en des fractions continues terminées par les mêmes quotients, il faut qu'elles soient liées l'une à l'autre par une équation de la forme

$$(3) \qquad x' = \frac{ax+b}{a'x+b'},$$

où a, b, a', b' désignent des entiers positifs ou négatifs satisfaisant à la condition

$$ab' - ba' = \pm 1. \tag{4}$$

Je dis maintenant que cette condition est suffisante. Pour le démontrer, remarquons d'abord qu'on peut supposer x et x' positives, car si l'une d'elles ou toutes deux sont négatives, on peut les remplacer par leurs valeurs absolues en changeant les signes de quelques-uns des coefficients a, b, a', b', changement qui n'altérera pas la condition (4).

Cela étant, on peut évidemment supposer a positif, car on ramènerait le cas contraire à celui-là en changeant les signes des quatre coefficients a, b, a', b'; quant à b, il peut être positif ou négatif. Si b est positif, a' et b' sont de même signe à cause de l'équation (4), et ils sont tous deux positifs à cause de l'équation (3), parce qu'on suppose x et x' positives. Si b est négatif, a' et b' sont de signes contraires à cause de l'équation (4); d'où il suit qu'en mettant en évidence les signes des nombres a, b, a', b', l'équation (3) a l'une des trois formes suivantes :

$$x' = \frac{ax + b}{a'x + b'},$$

$$x' = \frac{ax - b}{-a'x + b'},$$

$$x' = \frac{ax - b}{a'x - b'},$$

et, dans tous les cas, on a

$$ab' - ba' = \pm 1.$$

Dans le premier cas, on démontre aisément que x et x' se développent en des fractions continues terminées par les mêmes quotients (*voir* la seizième leçon). Le second cas se ramène au premier; car, en exprimant x en fonction de x', on trouve

$$x = \frac{b'x' + b}{a'x' + a}.$$

Pour démontrer que la même chose a lieu dans le troisième

cas, réduisons x en fraction continue. Soient $\frac{g}{g'}$ et $\frac{h}{h'}$ deux réduites consécutives aussi éloignées qu'on voudra, et z le quotient complet qui correspond à la réduite $\frac{h}{h'}$, on aura

$$x = \frac{hz + g}{h'z + g'},$$

et, par conséquent,

$$x' = \frac{(ah - bh')z + (ag - bg')}{(a'h - b'h')z + (a'g - b'g')} = \frac{cz + d}{c'z + d'};$$

on a d'ailleurs

$$cd' - dc' = (ab' - ba')(gh' - hg') = \pm 1;$$

le troisième cas se trouve donc ramené au premier, si les entiers c, d, c', d' sont positifs, ou du moins sont tous quatre de même signe. Or, c et d sont de même signe; en effet, ils ont respectivement le même signe que les différences

$$\frac{h}{h'} - \frac{b}{a}, \quad \frac{g}{g'} - \frac{b}{a},$$

lesquelles différences sont de même signe, puisque les fractions $\frac{h}{h'}$ et $\frac{g}{g'}$ diffèrent l'une de l'autre d'aussi peu qu'on veut. Pour une raison semblable, c' et d' sont de même signe, et parce que x' et z sont positives, on voit que les nombres c, d, c', d' sont de même signe; donc x' et z, par suite x' et x se développeront en des fractions continues terminées par les mêmes quotients.

Sur les fonctions linéaires de la forme $\frac{ax + b}{a'x + b'}$.

Soit posé

$$\theta x = \frac{ax + b}{a'x + b'}, \tag{1}$$

a, b, a', b' étant des quantités quelconques données; po-

sons aussi

$$\theta^2 x = \theta\theta x,\quad \theta^3 x = \theta\theta^2 x, \ldots,\quad \theta^m x = \theta\theta^{m-1} x;$$

il est très-aisé d'avoir l'expression générale de $\theta^m x$. Posons, en effet,

$$\theta^m x = \frac{a_m x + b_m}{a'_m x + b'_m}; \tag{2}$$

on pourra écrire, d'après la formation des fonctions $\theta^2 x$, $\theta^3 x$, etc.,

$$\left\{\begin{aligned} a_m &= a\, a_{m-1} + b\, a'_{m-1},\\ a'_m &= a' a_{m-1} + b' a'_{m-1},\\ b_m &= a b_{m-1} + b\, b'_{m-1},\\ b'_m &= a' b_{m-1} + b' b'_{m-1}. \end{aligned}\right. \tag{3}$$

Pour tirer de ces équations les valeurs de a_m, a'_m, b_m, b'_m en fonction des quantités connues a, a', b, b', désignons par z une quantité telle, que l'on ait

$$\frac{z}{1} = \frac{b + b'z}{a + a'z}, \tag{4}$$

on déduira des équations (3),

$$a_m + a'_m z = (a + a'z)(a_{m-1} + a'_{m-1} z),$$
$$b_m + b'_m z = (a + a'z)(b_{m-1} + b'_{m-1} z);$$

d'où l'on tire aisément

$$\left\{\begin{aligned} a_m + a'_m z &= (a + a'z)^m,\\ b_m + b'_m z &= z(a + a'z)^m. \end{aligned}\right. \tag{5}$$

En outre, comme l'équation (4) est du second degré, en appelant z et z' ses deux racines, on aura encore

$$\left\{\begin{aligned} a_m + a'_m z' &= (a + a'z')^m,\\ b_m + b'_m z' &= z'(a + a'z')^m. \end{aligned}\right. \tag{6}$$

Des équations (5) et (6) on peut maintenant tirer les valeurs de a_m; a'_m, b_m; b'_m.

En faisant, pour abréger,

(7) $$t = \sqrt{(a+b')^2 - 4(ab' - ba')},$$

et

(8) $$\begin{cases} P_m = (a+b'+t)^m + (a+b'-t)^m, \\ Q_m = \dfrac{(a+b'+t)^m - (a+b'-t)^m}{t}, \end{cases}$$

on trouve aisément

(9) $$\begin{cases} a_m = \dfrac{P_m + (a-b')Q_m}{2^{m+1}}, \\ a'_m = a'\dfrac{Q_m}{2^m}, \\ b_m = b\dfrac{Q_m}{2^m}, \\ b'_m = \dfrac{P_m - (a-b')Q_m}{2^{m+1}}, \end{cases}$$

équations dont on déduit

(10) $$\begin{cases} \dfrac{a_m - b'_m}{a'_m} = \dfrac{a-b'}{a'}, \\ \dfrac{b_m}{a'_m} = \dfrac{b}{a'}, \\ a_m b'_m - b_m a'_m = (ab' - ba')^m; \end{cases}$$

en sorte que, si

$$ab' - ba' = \pm 1,$$

on aura aussi

$$a_m b'_m - b_m a'_m = \pm 1.$$

On connaît donc les coefficients de la fonction $\theta^m x$ en fonction des quantités connues a, b, a', b'. A la vérité, notre analyse semble en défaut si t est nulle, car alors, z et z' étant égales, les équations (6) ne diffèrent pas des équations (5); mais, comme les équations (8) et (9) ont lieu quelque petite que soit t, elles seront vraies encore pour $t = 0$: on a, dans ce cas,

$$P_m = 2(a+b')^m,$$
$$Q_m = 2m(a+b')^{m-1},$$

et, par suite,

$$(11)\quad \begin{cases} a_m = \dfrac{(a+b')^m + m(a-b')(a+b')^{m-1}}{2^m}, \\ a'_m = \dfrac{ma'(a+b')^{m-1}}{2^{m-1}}, \\ b_m = \dfrac{mb(a+b')^{m-1}}{2^{m-1}}, \\ b'_m = \dfrac{(a+b')^m - m(a-b')(a+b')^{m-1}}{2^m}. \end{cases}$$

Ici, les quantités a, b, a', b' doivent vérifier l'équation

$$(12)\quad (a+b')^2 = 4(ab' - ba'),$$

et l'on peut écrire la valeur de $\theta^m x$ comme il suit :

$$\theta^m x = \frac{\left(a - b' + \dfrac{a+b'}{m}\right)x + 2b}{2a'x - \left(a - b' - \dfrac{a+b'}{m}\right)}.$$

On voit que, pour $m = \infty$, $\theta_m x$ converge vers la quantité

$$\frac{(a-b')x + 2b}{2a'x - (a-b')},$$

qui n'est autre chose que l'une des constantes $\frac{a-b'}{2a'}$, $\frac{-2b}{a-b'}$, lesquelles sont égales à cause de la relation (12).

Proposons-nous maintenant de trouver la condition nécessaire et suffisante pour que l'on ait identiquement

$$(13)\quad \theta_\mu x = x,$$

c'est-à-dire

$$(14)\quad a_\mu = b'_\mu, \quad a'_\mu = 0, \quad b_\mu = 0.$$

On voit immédiatement qu'on doit exclure le cas particulier où l'on aurait

$$(a+b')^2 = 4(ab' - ba'),$$

car les équations (11) indiquent que, pour satisfaire aux équations (14), il faudrait que l'on eût

$$a + b' = 0,$$

par suite,

$$ab' - ba' = 0,$$

et alors la fonction θx ne dépendrait pas de x. Cela étant, les équations (9) montrent que, pour satisfaire aux équations (14), il est nécessaire et suffisant que l'on ait

$$Q_\mu = 0,$$

ou

$$(a + b' + t)^\mu = (a + b' - t)^\mu.$$

On tire de là

$$a + b' + t = (a + b' - t)\left(\cos\frac{2\lambda\pi}{\mu} + \sqrt{-1}\sin\frac{2\lambda\pi}{\mu}\right)$$

et

(15) $$t = (a + b')\,\text{tang}\,\frac{\lambda\pi}{\mu}\sqrt{-1},$$

en désignant par λ un nombre entier qu'on doit supposer premier avec μ pour qu'il faille effectivement exécuter μ fois sur x l'opération désignée par θ avant de reproduire x.

En comparant cette valeur de t avec celle qu'on tire de l'équation (7), on a

(16) $$(a + b')^2 - 4(ab' - ba')\cos^2\frac{\lambda\pi}{\mu} = 0.$$

Telle est la condition nécessaire et suffisante pour que l'on ait identiquement

$$\theta^\mu x = x.$$

Si l'on suppose que a, b, a', b' soient réelles, l'équation (16) montre que la quantité $ab' - ba'$ doit être positive. Et comme on peut, sans changer la fonction θx, multiplier les constantes a, b, a', b' par un facteur quelconque, on voit que, sans faire aucune particularisation, on peut supposer

(17) $$ab' - ba' = 1;$$

alors l'équation (16) donne

(18) $$a + b' = 2\cos\frac{\lambda\pi}{\mu}.$$

Nous ne mettons pas le signe $\pm$ devant le second membre, parce qu'on peut, si on le juge à propos, changer les signes des quatre quantités a, b, a', b'.

Des équations (17) et (18) on tire

$$(19)\qquad \begin{cases} b' = -\left(a - 2\cos\dfrac{\lambda\pi}{\mu}\right), \\[2ex] b = -\dfrac{a^2 - 2a\cos\dfrac{\lambda\pi}{\mu} + 1}{a'}; \end{cases}$$

et la fonction θx a pour valeur

$$(20)\qquad \theta x = \frac{ax - \dfrac{a^2 - 2a\cos\dfrac{\lambda\pi}{\mu} + 1}{a'}}{a'x - \left(a - 2\cos\dfrac{\lambda\pi}{\mu}\right)}.$$

Les quantités a et a' demeurent indéterminées; quant à λ, c'est un nombre entier quelconque premier avec μ. Si l'on continue de poser

$$\theta^m x = \frac{a_m x + b_m}{a'_m x + b'_m},$$

on trouvera aisément

$$(21)\qquad \begin{cases} a_m = \dfrac{a\sin\dfrac{m\lambda\pi}{\mu} - \sin\dfrac{(m-1)\lambda\pi}{\mu}}{\sin\dfrac{\lambda\pi}{\mu}}, \\[3ex] a'_m = a'\dfrac{\sin\dfrac{m\lambda\pi}{\mu}}{\sin\dfrac{\lambda\pi}{\mu}}, \\[3ex] b_m = -\dfrac{a^2 - 2a\cos\dfrac{\lambda\pi}{\mu} + 1}{a'}\;\dfrac{\sin\dfrac{m\lambda\pi}{\mu}}{\sin\dfrac{\lambda\pi}{\mu}}, \\[3ex] b'_m = \dfrac{\sin\dfrac{(m+1)\lambda\pi}{\mu} - a\sin\dfrac{m\lambda\pi}{\mu}}{\sin\dfrac{\lambda\pi}{\mu}}. \end{cases}$$

Des équations (19) et (21) on déduit

$$(22)\quad \begin{cases} b'_m = -\left(a_m - 2\cos\dfrac{m\lambda\pi}{\mu}\right), \\ b_m = -\dfrac{a_m^2 - 2a_m\cos\dfrac{m\lambda\pi}{\mu} + 1}{a'_m}, \end{cases}$$

et

$$(23)\quad \begin{cases} a = \dfrac{a_m \sin\dfrac{\lambda\pi}{\mu} + \sin\dfrac{(m-1)\lambda\pi}{\mu}}{\sin\dfrac{m\lambda\pi}{\mu}}, \\ a' = a'_m \dfrac{\sin\dfrac{\lambda\pi}{\mu}}{\sin\dfrac{m\lambda\pi}{\mu}}, \\ b = -\dfrac{a_m^2 - 2a_m\cos\dfrac{m\lambda\pi}{\mu} + 1}{a^m} \dfrac{\sin\dfrac{\lambda\pi}{\mu}}{\sin\dfrac{m\lambda\pi}{\mu}}, \\ b' = \dfrac{\sin\dfrac{(m+1)\lambda\pi}{\mu} - a_m \sin\dfrac{\lambda\pi}{\mu}}{\sin\dfrac{m\lambda\pi}{\mu}}. \end{cases}$$

Ces formules permettent de résoudre la question suivante :

Étant donnée une fonction linéaire $\dfrac{a_m x + b_m}{a'_m x + b'_m}$, *trouver une fonction linéaire* $\theta x = \dfrac{ax + b}{a'x + b'}$, *telle, que l'on ait identiquement*

$$\theta^m x = \frac{a_m x + b_m}{a'_m x + b'_m} \quad \text{et} \quad \theta^\mu x = x.$$

On voit que le problème n'est possible que si les quantités données a_m, b_m, a'_m, b'_m satisfont aux équations (22).

Des équations irréductibles dont deux racines x et x' sont liées par la relation linéaire $x' = \dfrac{ax+b}{a'x+b'}$, où a, b, a', b' sont des constantes données.

Soit

$$(1) \qquad \chi(x) = 0$$

une équation irréductible, et supposons qu'entre deux racines x et x' on ait la relation

$$(2) \qquad x' = \frac{ax+b}{a'x+b'} = \theta x,$$

où a, b, a', b' sont des constantes données. On sait (vingt-sixième leçon) que toutes les quantités comprises dans la série indéfinie

$$x, \quad \theta x, \quad \theta^2 x, \quad \theta^3 x, \ldots,$$

doivent être racines de l'équation (1), ce qui exige que l'une des fonctions θx, $\theta^2 x$, etc., soit égale à x. Supposons

$$(3) \qquad \theta^{\mu} x = x.$$

Cette équation aura lieu identiquement, si l'on suppose que a, b, a', b' soient commensurables, ou, du moins, que ce soient des fonctions rationnelles des quantités que l'on considère comme connues, et dont dépendent rationnellement les coefficients de l'équation proposée. Par conséquent, d'après ce qu'on a vu précédemment, on peut écrire

$$(4) \qquad \begin{cases} b' = -\left(a - 2\cos\dfrac{\lambda\pi}{\mu}\right), \\[2ex] b = -\dfrac{a^2 - 2a\cos\dfrac{\lambda\pi}{\mu} + 1}{a'}, \end{cases}$$

en désignant toujours par λ un nombre entier premier avec μ.

Cela posé, on sait (vingt-sixième leçon) que le degré de l'équation (1) doit être un multiple $n\mu$ de μ, et que ses $n\mu$ racines

peuvent être représentées comme il suit :

$$(5)\quad \begin{cases} x, & \theta x; & \theta^2 x, \ldots, & \theta^{\mu-1} x, \\ x_1, & \theta x_1; & \theta^2 x_1, \ldots, & \theta^{\mu-1} x_1, \\ x_2, & \theta x_2, & \theta^2 x_2, \ldots, & \theta^{\mu-1} x_2, \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ x_{n-1}, & \theta x_{n-1}, & \theta^2 x_{n-1}, \ldots, & \theta^{\mu-1} x_{n-1}. \end{cases}$$

Soit

$$(6)\qquad x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x = y,$$

y dépendra d'une équation

$$(7)\qquad F(y) = 0$$

de degré n, et dont les coefficients seront des fonctions rationnelles des quantités connues de l'équation (1) et de la fonction θ. L'équation (7) peut n'être pas résoluble algébriquement, mais les quantités

$$x, \quad \theta x, \quad \theta^2 x, \ldots, \quad \theta^{\mu-1} x$$

dependent d'une équation de degré μ dont les coefficients sont des fonctions rationnelles de y, et qui est, comme on sait, toujours résoluble algébriquement. Dans le cas qui nous occupe, où la fonction θ est linéaire, cette dernière équation n'est autre que l'équation (6), et l'on voit, en résumé, que l'équation proposée (1) doit résulter de l'élimination de y entre les deux équations (6) et (7), dont la seconde peut être considérée comme ayant pour premier membre un polynôme irréductible quelconque de degré n.

En d'autres termes, les équations que nous étudions peuvent être considérées comme obtenues en multipliant un certain nombre n d'équations de la forme

$$\begin{gathered} x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y = 0, \\ x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y_1 = 0, \\ x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y_{n-1} = 0, \end{gathered}$$

où $y, y_1, y_2, \ldots, y_{n-1}$ désignent les n racines d'une équation irréductible dont les coefficients sont des quantités entièrement arbitraires.

Des équations irréductibles à coefficients numériques et dont deux ou plusieurs racines se développent en des fractions continues terminées par les mêmes quotients.

Cherchons maintenant dans quel cas les fractions continues, dans lesquelles se développent deux racines réelles x' et x d'une équation irréductible, sont terminées par les mêmes quotients.

Il faut et il suffit pour cela, comme on l'a vu plus haut, que l'on ait

$$x' = \frac{ax+b}{a'x+b'} = \theta x,$$

a, b, a', b' étant des entiers positifs ou négatifs liés par la relation

$$ab' - ba' = \pm 1;$$

en outre, pour que x et θx puissent représenter deux racines d'une équation irréductible, il faut qu'on puisse assigner un nombre entier μ, tel qu'on ait identiquement

$$\theta^{\mu} x = x,$$

ce qui exige, comme nous l'avons vu, qu'on ait

$$b' = -\left(a - 2\cos\frac{\lambda\pi}{\mu}\right),$$

$$b = -\frac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'},$$

λ étant un nombre entier premier avec μ. Or, puisque a, b, a', b' sont des nombres entiers, $2\cos\frac{\lambda\pi}{\mu}$ doit être un nombre entier, ce qui ne peut arriver que si μ est égal à 2 ou à 3. On voit par là que la propriété que nous étudions ne peut se ren-

contrer que chez les équations irréductibles dont le degré a la forme $2n$ ou la forme $3n$. Nous examinerons successivement ces deux classes d'équations.

Si l'on suppose $\mu = 2$ et $\lambda = 1$ (λ doit être premier avec μ), on a

$$\theta x = \frac{ax - \dfrac{a^2+1}{a'}}{a'x - a}$$

et

$$\theta^2 x = x;$$

a désigne un nombre entier quelconque, et n' un diviseur de $a^2 + 1$. Si l'on prend pour $F(y)$ un polynôme irréductible quelconque de degré n, et qu'on élimine y entre les deux équations

$$x + \theta x = y, \quad F(y) = 0,$$

ou

$$x^2 - yx + \left(\frac{ay}{n'} - \frac{n^2+1}{a'^2}\right) = 0, \quad F(y) = 0,$$

on aura la forme générale des équations de degré $2n$ jouissant de cette propriété, que les $2n$ racines se partageront en n groupes tels que, dans chaque groupe de deux racines réelles, les fractions continues qui représentent ces racines seront terminées par les mêmes quotients.

Ce résultat peut être énoncé d'une autre manière :

Soit a un nombre entier quelconque, n' un diviseur quelconque de $n^2 + 1$, y une quantité réelle quelconque commensurable ou incommensurable ; les deux racines de l'équation

$$x^2 - yx + \left(\frac{ay}{a'} - \frac{a^2+1}{n'^2}\right) = 0$$

se développeront en des fractions continues terminées par les mêmes quotients.

On déduit de là une conséquence assez remarquable, lorsque y est commensurable. On sait que, dans ce cas, les deux racines de l'équation précédente se développent en des fractions continues périodiques et que les périodes de ces deux fractions

continues sont formées des mêmes termes écrits en ordre inverse. D'où il suit que si la période de la fraction continue qui représente l'une des racines est, par exemple,

$$\alpha,\ \beta,\ \gamma,\ldots,\ \omega,$$

on pourra, si l'on veut, prendre pour période la suite inverse

$$\omega,\ldots,\ \gamma\ \ \beta,\ \alpha.$$

Supposons maintenant $\mu = 3$; on aura, en faisant $\lambda = 2$ (le cas de $\lambda = 1$ est identique à celui de $\lambda = 2$, on passe de l'un à l'autre en changeant les signes de a et a'),

$$\theta x = \frac{ax - \dfrac{a^2 + a + 1}{a'}}{a'x - (a+1)},$$

$$\theta^2 x = \frac{(a+1)x - \dfrac{a^2 + a + 1}{a'}}{a'x - a},$$

$$\theta^3 x = x;$$

a est un nombre entier quelconque, et a' un diviseur de $a^2 + a + 1$. Quelle que soit l'irrationnelle x, les fractions continues dans lesquelles se développent

$$x,\ \theta x,\ \theta^2 x,$$

se termineront pas les mêmes quotients. Si donc F (y) désigne un polynôme irréductible quelconque de degré n, et qu'on élimine y entre les équations

$$x + \theta x + \theta^2 x = y,\quad \mathrm{F}(y) = 0,$$

on

$$\left\{\begin{aligned} & x^3 - yx^2 + \left[\frac{(2a+1)y}{a'} - \frac{3(a^2+a+1)}{a'^2}\right]x \\ & \quad - \left[\frac{a(a+1)y}{a'^2} - \frac{(2a+1)(a^2+a+1)}{a'^3}\right] = 0, \\ & \mathrm{F}(y) = 0, \end{aligned}\right.$$

on obtiendra l'expression générale des équations de degré $3n$ qui jouissent de la propriété, que les $3n$ racines se partageront

en n groupes tels que, dans chaque groupe de trois racines réelles, les fractions continues qui représentent ces racines seront terminées par les mêmes quotients.

On voit, en particulier, que les équations du troisième degré qui ont cette propriété sont comprises dans la forme générale suivante :

$$x^3 - yx^2 + \left[\frac{(2a+1)y}{a'} - \frac{3(a^2+a+1)}{a'^2}\right]x - \left[\frac{a(a+1)y}{a'^2} - \frac{(2a+1)(a^2+a+1)}{a'^3}\right] = 0,$$

où a désigne un entier quelconque, a' un diviseur quelconque de $a^2 + a + 1$, et y une quantité quelconque, commensurable ou incommensurable. En faisant $y = 0$, on obtient la solution du cas particulier que M. Lobatto a examiné.

Les équations du troisième degré qui proviennent de la division du cercle en sept ou neuf parties égales, celle du quatrième degré qui provient de la division en quinze parties égales, jouissent de la propriété remarquable qu'on vient d'étudier.

La division du cercle en sept parties égales conduit à l'équation

$$x^3 + x^2 - 2x - 1 = 0,$$

et si l'on représente par x la racine positive, par $-x_1$ et $-x_2$ les deux racines négatives, on a

$$x_1 = \frac{1}{1+x}, \quad x_2 = 1 + \frac{1}{x};$$

la racine x est comprise entre 1 et 2, on aura par conséquent des résultats de cette forme :

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{6 + \dots}} \qquad x_1 = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{6 + \dots}}}$$

$$x_2 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6 + \dots}}}$$

La division du cercle en neuf parties égales conduit à l'équation

$$x^3 - 3x + 1 = 0$$

Si l'on désigne par $-x$ la racine négative, laquelle est comprise entre -1 et -2, par x_1 et x_2 les deux racines positives, on a

$$x_1 = \frac{1}{1+x}, \quad x_2 = 1 + \frac{1}{x},$$

ce qui conduit aux mêmes résultats que le cas précédent.

Enfin, l'équation du quatrième degré dont dépend la division du cercle en quinze parties égales, est

$$x^4 - x^3 - 4x^2 + 4x + 1 = 0.$$

Si x et x_1 désignent les deux racines positives, $-x'$ et $-x'_1$ les deux négatives, on a

$$x = \frac{x'+2}{x'+1} = 1 + \frac{1}{1+x'},$$
$$x_1 = \frac{x'_1+2}{x'_1+1} = 1 + \frac{1}{1+x'_1}.$$

Des deux quantités x' et x'_1 l'une est comprise entre 0 et 1, l'autre entre 1 et 2; on aura donc des résultats de cette forme:

$$x' = \cfrac{1}{\alpha + \cfrac{1}{6 + \dots}} \qquad x = 1 + \cfrac{1}{1 + \cfrac{1}{\alpha + \cfrac{1}{6 + \dots}}}$$

$$x'_1 = 1 + \cfrac{1}{\alpha' + \cfrac{1}{6' + \dots}} \qquad x_1 = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha' + \cfrac{1}{6' + \dots}}}$$

L'équation que nous considérons résulte de l'élimination de y entre

$$x + \frac{x-2}{x-1} = y, \quad y^2 - y - 1 = 0.$$

NOTE VIII.

SUR LE NOMBRE DES VALEURS QUE PEUT PRENDRE UNE FONCTION QUAND ON Y PERMUTE LES LETTRES QU'ELLE RENFERME.

Je me propose, dans cette Note, de donner un extrait des deux Mémoires que j'ai publiés dans le tome XV du Journal de M. Liouville et qui contiennent l'ensemble de mes recherches sur le nombre des valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. Je me bornerai ici à démontrer rigoureusement et sans recourir à aucun postulatum, les deux théorèmes suivants :

1°. *Une fonction de n lettres qui a moins de n valeurs n'en a que deux au plus, si n est > 4;*

2°. *Une fonction de n lettres qui a précisément n valeurs est symétrique par rapport à $n-1$ lettres, sauf le seul cas de $n = 6$.*

Les seules propositions connues sur lesquelles nous aurons à nous appuyer sont les deux suivantes :

1°. *Si V est une fonction de n lettres $a, b, c, \ldots, k, l$ qui prend μ valeurs distinctes $V_1, V_2, \ldots, V_\mu$ quand on y permute les lettres a, b, etc., toute fonction symétrique de $V_1, V_2, \ldots, V_\mu$ est également une fonction symétrique des lettres $a, b, c, \ldots, k, l$.*

2°. *Si une fonction d'un nombre n de lettres supérieur à 3 n'a que deux valeurs par les permutations de $n-1$ lettres, elle a 2 ou $2n$ valeurs par les permutations de toutes les lettres.*

Ces propositions ont été démontrées, l'une dans la troisième leçon, l'autre dans la vingtième.

LEMME I. — *Soient*

$$V_1, \; V_2, \ldots, \; V_\mu$$

μ fonctions de n lettres $a, b, c, d, \ldots, k, l$: si les coefficients de l'équation

$$(1) \qquad (x - V_1)(x - V_2)\ldots(x - V_\mu) = 0,$$

ordonnée par rapport aux puissances de x, sont des fonctions symétriques des n lettres a, b, c, d,..., k, l, la fonction V_1 ne pourra acquérir par les permutations de ces n lettres que des valeurs faisant partie de la série

$$V_1,\ V_2,\ldots,\ V_\mu.$$

En effet, faisons subir aux lettres a, b, c, d,..., k, l une permutation quelconque, l'équation (1) ne changera pas, puisque ses coefficients sont des fonctions symétriques; donc ses racines ne changeront pas non plus.

Ainsi, en faisant une permutation quelconque, les fonctions

$$V_1,\ V_2,\ldots,\ V_\mu$$

sont invariables, ou se changent les unes dans les autres. Ce qu'il fallait démontrer.

Lemme II. — *Si une fonction de n lettres a $\mu + \nu$ valeurs, et qu'elle ne prenne que μ valeurs distinctes par les permutations de m lettres, il y aura aussi m lettres parmi les n que contient la fonction, dont les permutations lui feront acquérir un nombre de valeurs distinctes égal ou inférieur à ν.*

Soit

$$V = \varphi(a,\ b,\ c,\ d,\ldots,\ k,\ l)$$

une fonction de n lettres ayant $\mu + \nu$ valeurs, et supposons que par les permutations des m lettres

$$g,\ h,\ldots,\ k,\ l,$$

la fonction V ne prenne que les μ valeurs

$$V_1,\ V_2,\ldots,\ V_\mu.$$

Soient aussi

$$V_{\mu+1},\ V_{\mu+2},\ldots,\ V_{\mu+\nu}$$

les ν autres valeurs dont V est susceptible.

Les coefficients de l'équation

$$(x - V_1)(x - V_2)\ldots(x - V_{\mu+\nu}) = 0$$

sont des fonctions symétriques des n lettres $a, b, c, d, \ldots, k, l$; pareillement les coefficients de l'équation

$$(x - V_1)(x - V_2)\ldots(x - V_\mu) = 0$$

sont des fonctions symétriques des m lettres $g, h, \ldots, k, l$; donc l'équation qu'on obtient en divisant les deux précédentes, savoir,

$$(x - V_{\mu+1})(x - V_{\mu+2})(x - V_{\mu+\nu}) = 0,$$

a aussi pour coefficients des fonctions symétriques de $g, h, \ldots, k, l$. Par conséquent, d'après le lemme I, les valeurs que la fonction $V_{\mu+1}$ peut prendre, par les permutations des lettres $g, h, \ldots, k, l$, font partie des ν suivantes,

$$V_{\mu+1},\ V_{\mu+2},\ V_{\mu+\nu};$$

donc, parmi les n lettres qui entrent dans la fonction V, il y en a m dont les permutations font acquérir à cette fonction un nombre de valeurs distinctes égal ou inférieur à ν.

COROLLAIRE. — *Si une fonction de n lettres a μ valeurs distinctes, dont $\mu - 1$ seulement peuvent être obtenues par les permutations de m lettres, la fonction est symétrique par rapport à m lettres.*

LEMME III. — *Si une fonction non symétrique de n lettres, n étant > 4, est symétrique par rapport à $n - 2$ lettres, le nombre des valeurs distinctes de la fonction est n, $\frac{n(n-1)}{2}$ ou $n(n-1)$.*

Soit

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres, symétrique par rapport aux $n - 2$ lettres

$$c, d, \ldots, k, l.$$

1°. Si cette fonction ne change pas de valeurs par la transposition de l'une des lettres a et b, b par exemple, avec l'une des $n - 2$ autres, elle sera symétrique par rapport aux $n - 1$ lettres

$$b, c, d, \ldots, k, l;$$

et comme, par hypothèse, elle n'est pas symétrique par rapport aux n lettres, elle aura précisément n valeurs.

2°. Supposons que la fonction V change par la transposition de l'une quelconque des deux lettres a et b avec l'une des $n-2$ autres, et qu'elle ne soit pas symétrique par rapport aux deux lettres a et b.

On formera évidemment toutes les valeurs dont la fonction V est susceptible, en faisant les $n(n-1)$ arrangements deux à deux des n lettres

$$a, b, c, d, \ldots, k, l,$$

et permutant dans la valeur de V les deux lettres a et b successivement avec les deux lettres de chacun de ces arrangements. Or je dis que toutes les valeurs de V formées ainsi sont différentes.

En effet, les deux valeurs de V qui correspondent à deux arrangements formés des mêmes lettres, a, b et b, a par exemple, ne peuvent être égales, puisque l'égalité

$$\varphi(a, b, c, d, \ldots, k, l) = \varphi(b, a, c, d, \ldots, k, l)$$

exige que la fonction V soit symétrique par rapport à a et b, ce qui est contre l'hypothèse.

Pareillement, les deux valeurs de V qui correspondent à deux arrangements ayant une lettre commune, tels que a, b et a, c, ou a, b et c, a sont différentes. En d'autres termes, on ne peut avoir

$$\varphi(a, b, c, d, \ldots, k, l) = \varphi(a, c, b, d, \ldots, k, l),$$

ni

$$\varphi(a, b, c, d, \ldots, k, l) = \varphi(c, a, b, d, \ldots, k, l).$$

L'impossibilité de ces égalités résulte de ce que le premier membre de chacune d'elles est symétrique par rapport aux deux lettres c et d, tandis que le second ne l'est pas par hypothèse.

Enfin les deux valeurs de V qui correspondent à deux arrangements a, b et c, d qui n'ont aucune lettre commune, sont aussi différentes; on ne peut avoir

$$\varphi(a, b, c, d, \ldots, k, l) = \varphi(c, d, a, b, \ldots, k, l),$$

parce que le premier membre est symétrique par rapport à c et d, tandis que le second ne l'est pas.

On voit donc que le nombre des valeurs distinctes de V est $n(n-1)$.

3°. Supposons, enfin, que la fonction V change par la transposition de l'une quelconque des lettres a et b avec l'une des $n-2$ autres, mais qu'elle soit symétrique par rapport aux deux lettres a et b.

Dans ce cas, on formera toutes les valeurs de V en faisant les $\frac{n(n-1)}{2}$ combinaisons deux à deux des n lettres

$$a, b, c, d, \ldots, k, l,$$

et permutant dans la valeur de V les deux lettres a et b successivement avec les deux lettres de chacune de ces combinaisons. Or je dis que toutes les valeurs de V ainsi formées seront différentes si n est supérieur à 4.

En effet, deux valeurs de V qui correspondent à deux combinaisons a, b et a, c, qui ont une lettre commune, sont différentes; on ne peut avoir

$$\varphi(a, b, c, d, \ldots, k, l) = \varphi(a, c, b, d, \ldots, k, l),$$

parce que le premier membre est symétrique par rapport à a et b, et que le second ne l'est pas par hypothèse.

Pareillement, deux valeurs de V qui correspondent à deux combinaisons a, b et c, d, qui n'ont aucune lettre commune, sont aussi différentes; en d'autres termes, on ne peut avoir

$$\varphi(a, b, c, d, \ldots, k, l) = \varphi(c, d, a, b, \ldots, k, l),$$

parce que le premier membre est symétrique par rapport aux $n-2$ lettres c, d, ..., k, l, et que le second ne l'est pas par hypothèse si n est > 4.

On voit donc que le nombre des valeurs distinctes de V est $\frac{n(n-1)}{2}$.

Remarque. — La démonstration de ce dernier cas suppose

essentiellement $n > 4$; car si l'on a $n = 4$, on ne peut plus dire que l'égalité

$$\varphi(a, b, c, d) = \varphi(c, d, a, b)$$

soit impossible. Cette égalité peut, au contraire, avoir lieu; cela arrive en particulier pour la fonction

$$ab + cd,$$

et pour une infinité d'autres.

Corollaire. — *Si une fonction de n lettres, symétrique par rapport à n — 2 lettres, a n valeurs, elle est symétrique par rapport à n — 1 lettres.*

Lemme IV. — *Si une fonction de n lettres, n étant* > 4, *a deux valeurs seulement par les permutations de n — 2 lettres, le nombre des valeurs que cette fonction peut prendre par les permutations de toutes les lettres est égal à 2, ou supérieur à n.*

Soit

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres, n étant > 4, qui n'a que deux valeurs par les permutations des $n - 2$ lettres

$$c, \; d, \ldots, \; k, \; l.$$

D'après la proposition démontrée dans la vingtième leçon et rappelée plus haut, comme on suppose $n - 1 > 3$, la fonction V aura 2 ou $2(n-1)$ valeurs par les permutations des $n - 1$ lettres

$$b, \; c, \; d, \ldots, \; k, \; l.$$

Si le dernier cas a lieu, le nombre total des valeurs de V est supérieur à n. Si, au contraire, la fonction V n'a que deux valeurs par les permutations des $n - 1$ lettres

$$b, \; c, \; d, \ldots \; k, \; l,$$

elle en aura 2 ou $2 \cdot n$ par les permutations de toutes les lettres.

La proposition est donc démontrée.

Lemme V. — *Si une fonction de n lettres, non symétrique, a un nombre impair de valeurs distinctes, il est impossible*



qu'elle prenne toutes les valeurs dont elle est susceptible, par les seules permutations de $n-2$ lettres.

Soit

$$V=\varphi(a,\ b,\ c,\ d,\ldots,\ k,\ l)$$

une fonction de n lettres ayant un nombre impair μ de valeurs distinctes, et supposons qu'elle puisse prendre ses μ valeurs par les seules permutations des $n-2$ lettres

$$c,\ d,\ldots,\ k,\ l.$$

Représentons ces μ valeurs par

$$(1)\quad \varphi_1(a,\ b,\ldots),\ \varphi_2(a,\ b,\ldots),\ldots,\ \varphi_\mu(a,\ b,\ldots).$$

Il est d'abord évident que la fonction V ne peut être symétrique par rapport aux lettres a et b; car toutes les valeurs qu'elle peut prendre étant symétriques par rapport à a et b, le seraient également par rapport à deux lettres choisies à volonté, qu'on peut introduire, par une substitution, à la place de a et de b. La fonction V serait donc symétrique, ce qui est contre l'hypothèse.

Cela posé, faisons dans les fonctions (1) la transposition $(a,\ b)$, elles deviennent

$$(2)\quad \varphi_1(b,a,\ldots),\ \varphi_2(b,a,\ldots),\ldots,\ \varphi_\mu(b,a,\ldots).$$

Les fonctions (1) étant distinctes par hypothèse, les fonctions (2) le sont aussi, et comme la série (1) comprend toutes les valeurs de V, les fonctions (2) ne différeront pas des fonctions (1); d'ailleurs les termes qui occupent le même rang dans ces suites ne peuvent être égaux, puisque la fonction V n'est pas symétrique par rapport à a et b. Supposons donc que l'on ait

$$\varphi_1(a,b,\ldots)=\varphi_\mu(b,a,\ldots);$$

en changeant a et b l'une avec l'autre, il vient

$$\varphi_1(b,a,\ldots)=\varphi_\mu(a,b,\ldots);$$

d'où il suit que les termes de la suite (1) peuvent être groupés

deux à deux, de manière que les deux termes d'un même groupe se changent l'un dans l'autre, par la transposition (a, b). Or, cela est impossible, puisque μ est un nombre impair. La proposition est donc démontrée.

Lemme VI. — *Si une fonction de n lettres*

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

prend toutes ses valeurs par les seules permutations des $n-2$ lettres

$$c, d, \ldots, k, l,$$

le nombre de ces valeurs est double du nombre des valeurs que prend la fonction

$$X = [x - \varphi(a, b, c, d, \ldots, k, l)][x - \varphi(b, a, c, d, \ldots, k, l)],$$

par les permutations des $n-2$ lettres $c, d, \ldots, k, l$.

On voit, comme dans la proposition précédente, que la fonction V ne peut être symétrique par rapport aux lettres a et b, et que les valeurs de V peuvent être groupées deux à deux, de manière que les termes d'un même groupe se changent l'un dans l'autre par la transposition (a, b). Il résulte de là que les valeurs de V peuvent être partagées en deux séries de la manière suivante :

$$\varphi_1(a, b), \varphi_2(a, b), \ldots, \varphi_\mu(a, b),$$
$$\varphi_1(b, a), \varphi_2(b, a), \ldots, \varphi_\mu(b, a).$$

Cela posé, la fonction X ne peut acquérir que les μ valeurs suivantes, par les permutations des $n-2$ lettres $c, d, \ldots, k, l$,

$$[x - \varphi_1(a, b)][x - \varphi_1(b, a)],$$
$$[x - \varphi_2(a, b)][x - \varphi_2(b, a)),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[x - \varphi_\mu(a, b)][x - \varphi_\mu(b, a)];$$

car toute permutation des lettres $c, d, \ldots, k, l$ qui laisse $\varphi_1(a, b)$ invariable, ou qui la change en $\varphi_1(b, a)$, laisse invariable $\varphi_1(b, a)$ ou la change en $\varphi_1(a, b)$; et de même toute permutation des

lettres c, d, ..., k, l qui change $\varphi_1(a, b)$ en $\varphi_2(a, b)$ ou en $\varphi_2(b, a)$ change aussi $\varphi_1(b, a)$ en $\varphi_2(b, a)$ ou en $\varphi_2(a, b)$.

De plus, les μ valeurs de X, ecrites plus haut, sont différentes, car s'il n'y en avait que μ' de distinctes, μ' étant $< \mu$, en multipliant ces μ' valeurs et égalant à zéro le produit, on aurait une équation dont le premier membre serait une fonction symétrique des $n-2$ lettres $c, d, \ldots, k, l$, et dont les $2\mu'$ racines seraient les seules valeurs distinctes de la fonction V (lemme I), ce qui est impossible, puisqu'on a supposé ce nombre de valeurs égal à 2μ.

Il est donc démontré que le nombre des valeurs de la fonction V est double du nombre des valeurs que peut prendre la fonction X par les permutations des $n-2$ lettres $c, d, \ldots, k, l$.

THÉORÈME I. — *Une fonction d'un nombre impair n de lettres, qui a moins de n valeurs distinctes, ne peut en avoir plus de deux.*

Je vais démontrer généralement que si le théorème a lieu pour les fonctions de $n-2$ lettres, il a lieu aussi pour les fonctions de n lettres; et comme il est évidemment vrai pour les fonctions de trois lettres, il sera vrai aussi pour les fonctions de cinq, de sept, etc., d'un nombre impair quelconque de lettres.

Soit

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres qui a moins de n valeurs distinctes, n étant un nombre impair au moins égal à 5.

Soient a et b deux lettres quelconques, et faisons toutes les permutations des $n-2$ autres lettres

$$c, d, \ldots, k, l,$$

sans changer la place ni de a ni de b; comme nous admettons qu'une fonction de $n-2$ lettres qui a moins de $n-2$ valeurs, ne peut en avoir plus de deux, le nombre des valeurs de V résultant des permutations des $n-2$ lettres $c, d, \ldots, k, l$ sera nécessairement l'un des quatre suivants :

$$1,\ 2,\ n-2,\ n-1.$$

Nous allons faire successivement ces quatre hypothèses.

1°. *La fonction V est symétrique par rapport aux $n-2$ lettres $c, d, \ldots, k, l$.*

Alors elle aura, d'après le lemme III, n ou $\frac{n(n-1)}{2}$, ou $n(n-1)$ valeurs distinctes. Cette hypothèse n'est donc pas admissible, puisque V a moins de n valeurs.

2°. *La fonction V a deux valeurs par les permutations des $n-2$ lettres $c, d, \ldots, k, l$.*

Alors, d'après le lemme IV, la fonction V n'a en tout que deux valeurs, puisqu'elle en a moins de n.

3°. *La fonction V a $n-2$ valeurs par les permutations des $n-2$ lettres $c, d, \ldots, k, l$.*

Alors, d'après le lemme V, il est impossible que la fonction V n'ait que $n-2$ valeurs par les permutations des n lettres, parce que $n-2$ est un nombre impair; elle en a donc $n-1$. Mais alors, d'après le lemme II (corollaire), la fonction V est symétrique par rapport à $n-2$ lettres, et, par conséquent, elle a n, $\frac{n(n-1)}{2}$ ou $n(n-1)$ valeurs. Cette hypothèse est donc inadmissible.

4°. *La fonction V a $n-1$ valeurs par les permutations des $n-2$ lettres $c, d, \ldots, k, l$.*

Comme la fonction V n'a en tout que $n-1$ valeurs, la fonction

$$X = [x - \varphi(a, b, c, d, \ldots, k, l)][x - \varphi(b, a, c, d, \ldots, k, l)]$$

a $\frac{n-1}{2}$ valeurs par les permutations des $n-2$ lettres $c, d, \ldots, k, l$ (lemme VI). Mais on a

$$\frac{n-1}{2} < n-2,$$

et nous admettons qu'une fonction de $n-2$ lettres qui a moins de $n-2$ valeurs, n'en a au plus que deux ; donc la fonction X a une ou deux valeurs seulement, et, par conséquent, on doit

avoir

$$\frac{n-1}{2} = 1 \quad \text{ou} \quad = 2,$$

c'est-à-dire

$$n = 3 \quad \text{ou} \quad n = 5.$$

Nous avons supposé $n > 3$, donc l'hypothèse que nous discutons en ce moment est inadmissible, à moins que n ne soit égal à 5. Mais elle l'est encore dans ce cas, car une fonction de cinq lettres ne peut avoir quatre valeurs par les permutations de trois lettres, à cause que 4 n'est pas un diviseur du produit 1.2.3.

Conclusion. — On voit que la seconde de nos quatre hypothèses est seule admissible, et, par conséquent, si la fonction V a moins de n valeurs, elle ne peut en avoir plus de deux.

Théorème II. — *Une fonction d'un nombre impair n de lettres, qui a précisément n valeurs, est symétrique par rapport à n — 1 lettres.*

La démonstration suivante suppose n au moins égal à 5, mais pour les fonctions de trois lettres, le théorème est presque évident (*).

Soit

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

une fonction d'un nombre impair n de lettres, qui a précisément n valeurs.

Soient a et b deux lettres quelconques, et faisons toutes les permutations des $n-2$ autres lettres

$$c,\ d, \ldots,\ k,\ l;$$

il en résultera pour V un nombre de valeurs qui sera l'un des suivants

$$1,\ 2,\ 3, \ldots,\ (n-2),\ (n-1),\ n.$$

Mais, d'après le théorème I, $n-2$ étant impair, si ce nombre

(*) Le théorème a été démontré dans la vingtième leçon pour les fonctions de trois lettres.

de valeurs est inférieur à $n-2$, il est au plus égal à 2, ce sera donc l'un des cinq nombres

$$1,\ 2,\ n-2,\ n-1,\ n.$$

Nous allons faire ces cinq hypothèses.

1°. *La fonction* V *est symétrique par rapport aux* $n-2$ *lettres* $c, d, \ldots, k, l$.

Alors, d'après le lemme III, le nombre des valeurs de V ne peut être égal à n que si cette fonction est symétrique par rapport à $n-1$ lettres.

2°. *La fonction* V *a deux valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Cela est impossible d'après le lemme IV.

3°. *La fonction* V *a* $n-2$ *valeurs par les permutations des* $n-2$ lettres $c, d, \ldots, k, l$.

Alors, d'après le lemme II, la fonction V ayant en tout n valeurs et n'en ayant que $n-2$ par les permutations de $n-2$ lettres, il y a $n-2$ lettres dont les permutations font acquérir à V un nombre de valeurs égal à 1 ou à 2. Par conséquent, le nombre des valeurs de cette fonction ne peut être égal à n, que si elle est symétrique par rapport à $n-1$ lettres.

4°. *La fonction* V *a* $n-1$ *valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Alors, d'après le lemme II, la fonction V est symétrique par rapport à $n-2$ lettres, et, par conséquent, elle ne peut avoir n valeurs que si elle est symétrique par rapport à $n-1$ lettres, d'après le lemme III.

5°. *La fonction* V *prend ses* n *valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Cela est impossible, d'après le lemme V, parce que n est un nombre impair.

Conclusion. — La première, la troisième et la quatrième hypothèse sont, comme on voit, seules admissibles, et quelle que soit celle qui a lieu, la fonction V est nécessairement symétrique par rapport à $n-1$ lettres; ce qu'il fallait démontrer.

Théorème III. — *Une fonction d'un nombre pair n de lettres qui*

a moins de n valeurs ne peut en avoir plus de deux, si n est supérieur à 4.

Ce théorème n'a pas lieu pour les fonctions de quatre lettres; et c'est précisément parce qu'on peut former des fonctions de quatre lettres qui n'ont que trois valeurs, qu'on peut résoudre l'équation générale du quatrième degré.

Soit

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

une fonction d'un nombre n de lettres pair et supérieur à 4, et supposons que cette fonction ait moins de n valeurs.

Si l'on considère V comme fonction des $n-1$ lettres

$$b, c, d, \ldots, k, l,$$

et qu'on permute ces lettres, on obtiendra un nombre de valeurs distinctes de V, qui, étant par hypothèse inférieur à n, sera l'un des suivants

$$1, 2, 3, \ldots, n-2, n-1.$$

Mais, d'après le théorème I, comme $n-1$ est impair, ce nombre de valeurs ne peut s'abaisser au-dessous de $n-1$, sans être égal à 2 ou à 1; donc le nombre des valeurs distinctes de V résultant des permutations des $n-1$ lettres $b, c, d, \ldots, k, l$ est l'un des trois suivants :

$$1, 2, n-1.$$

Examinons ces trois cas.

1°. *La fonction* V *est symétrique par rapport aux* $n-1$ *lettres* $b, c, d, \ldots, k, l$.

Alors, elle a évidemment n valeurs, ce qui est contre l'hypothèse; à moins qu'elle ne soit symétrique par rapport à toutes les lettres, et, dans ce cas, elle n'a qu'une seule valeur.

2°. *La fonction* V *a deux valeurs par les permutations des* $n-1$ *lettres* $b, c, d, \ldots, k, l$.

Alors, d'après la proposition démontrée dans la vingtième leçon et déjà rappelée, la fonction V ayant moins de n valeurs, ne peut en avoir que deux.

3°. *La fonction* V *a* $n-1$ *valeurs par les permutations des* $n-1$ *lettres* $b, c, d, \ldots, k, l$.

Dans ce cas, comme $n-1$ est impair, la fonction V est symétrique par rapport à $n-2$ lettres, d'après le théorème II, et alors, d'après le lemme III, elle a au moins n valeurs.

Conclusion. — Puisqu'on suppose que V a moins de n valeurs, et que cette fonction n'est pas symétrique, le second des trois cas précédents est seul possible, et alors la fonction V a deux valeurs seulement. Ce qu'il fallait démontrer.

Théorème IV. — *Si une fonction d'un nombre n de lettres pair et supérieur à* 6 *a n valeurs, elle est symétrique par rapport à* $n-1$ *lettres.*

Soit

$$V = \varphi(a, b, c, d, \ldots, k, l)$$

une fonction de n lettres qui a précisément n valeurs. On suppose n pair et supérieur à 6.

Soient a et b deux lettres quelconques, et permutons les $n-2$ autres lettres

$$c,\ d, \ldots,\ k,\ l.$$

Le nombre des valeurs qu'on obtiendra ainsi pour V ne pouvant, d'après le théorème III, être à la fois plus grand que 2 et moindre que $n-2$ (puisque, par hypothèse, $n-2$ est > 4), sera l'un des cinq suivants :

$$1,\ 2,\ n-2,\ n-1,\ n.$$

Nous allons faire ces cinq hypothèses.

1°. *La fonction* V *est symétrique par rapport aux* $n-2$ *lettres* $c, d, \ldots, k, l$.

Alors, d'après le lemme III, elle ne peut avoir n valeurs que si elle est symétrique par rapport à $n-1$ lettres.

2°. *La fonction* V *a deux valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Cela est impossible d'après le lemme IV; car, alors, la fonction V n'aurait, en tout, que deux valeurs, ou elle en aurait plus de n.

3°. *La fonction* V *a* $n-2$ *valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Alors la fonction V ayant en tout n valeurs, elle a une ou deux valeurs seulement par les permutations de $n-2$ lettres (lemme II), et, par conséquent, elle ne peut en avoir n en tout que si elle est symétrique par rapport à $n-1$ lettres (lemmes III et IV).

4°. *La fonction* V n $n-1$ *valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Dans ce cas, d'après le lemme II, V est symétrique par rapport à $n-2$ lettres, et, par conséquent, elle ne peut avoir n valeurs que si elle est symétrique par rapport à $n-1$ lettres.

5°. *La fonction* V *a* n *valeurs par les permutations des* $n-2$ *lettres* $c, d, \ldots, k, l$.

Cela est impossible d'après le lemme VI, car alors la fonction

$$[x-\varphi(a, b, c, d, \ldots, k, l)][x-\varphi(b, a, c, d, \ldots, k, l)]$$

aurait, par les permutations des $n-2$ lettres $c, d, \ldots, k, l$, un nombre de valeurs égal à $\frac{n}{2}$, ce qui ne peut être, puisque $\frac{n}{2}$ est $< n-2$ et > 2.

Conclusion. — Le premier, le troisième et le quatrième cas sont seuls possibles, et l'on voit que le nombre des valeurs de la fonction V ne peut être égal à n, que si V est symétrique par rapport à $n-1$ lettres.

Remarque. — La démonstration ne s'applique pas aux fonctions de quatre et de six lettres; mais le théorème a été démontré dans la vingtième leçon pour les fonctions de quatre lettres, et il n'a pas lieu pour les fonctions de six lettres.

Des fonctions de six lettres qui ont six valeurs et qui ne sont pas symétriques par rapport à cinq lettres.

Dans la théorie qui vient d'être exposée, les fonctions de six lettres constituent une exception digne de remarque; aussi je crois devoir indiquer, en terminant cette Note, la composition des fonctions de six lettres qui ont six valeurs distinctes et qui ne sont pas cependant symétriques par rapport à cinq lettres.

Je dis en premier lieu que :

Si une fonction de six lettres, non symétrique par rapport à cinq lettres, a précisément six valeurs distinctes, cette fonction prend ses six valeurs par les seules permutations de trois lettres quelconques.

Soit V une pareille fonction des six lettres

$$a,\ b,\ c,\ d,\ e,\ f;$$

nous diviserons la démonstration du théorème énoncé en trois parties :

1°. Le nombre des valeurs que prend V par les permutations de cinq lettres quelconques

$$b,\ c,\ d,\ e,\ f$$

est un diviseur du produit 1.2.3.4.5; d'ailleurs ce nombre, qui est au plus égal à 6, ne peut s'abaisser au-dessous de 5 sans être égal à 1 ou à 2; donc la fonction V a 1, 2, 5 ou 6 valeurs par les permutations des cinq lettres. Mais si ce nombre de valeurs était 1 ou 5, la fonction V serait symétrique par rapport à cinq des six lettres a, b, c, d, e, f (lemme II), ce qui est contraire à l'hypothèse; si le même nombre était 2, la fonction V aurait 2 ou 12 valeurs (vingtième leçon) par les permutations des six lettres. Donc la fonction V doit prendre ses 6 valeurs par les seules permutations des cinq lettres b, c, d, e, f.

2°. Le nombre des valeurs que prend V par les permutations de quatre lettres quelconques

$$c,\ d,\ e,\ f$$

est un diviseur du produit 1.2.3.4; d'ailleurs ce nombre est au plus égal à 6; donc la fonction V a 1, 2, 3, 4 ou 6 valeurs par les permutations des quatre lettres. Si ce nombre était 1, la fonction V aurait 1 ou 5 valeurs par les permutations des cinq lettres b, c, d, e, f, ce qui n'a pas lieu; s'il était 2, la fonction V aurait 2 ou 10 valeurs par les permutations des cinq lettres; s'il était 4, la fonction V aurait au plus 2 valeurs par les permutations de quatre des cinq lettres b, c, d, e, f (lemme II), et nous venons de voir que cela est impossible. Nous allons prouver enfin que 3 ne peut exprimer le nombre des valeurs que

prend V par les permutations des quatre lettres c, d, e, f. En effet, nommons V_1, V_2, V_3, V_4, V_5, V_6 les six valeurs de V et supposons que cette fonction ne prenne que les valeurs V_1, V_2, V_3 par les permutations des quatre lettres c, d, e, f. La fonction

$$X = (x - V_1)(x - V_2)(x - V_3)$$

sera symétrique par rapport à c, d, e, f, et, par suite, elle aura 1 ou 5 valeurs par les permutations de b, c, d, e, f. Le premier cas ne peut avoir lieu (lemme I), car V n'aurait d'autres valeurs que V_1, V_2, V_3 par les permutations des cinq lettres b, c, d, e, f. La fonction X a donc 5 valeurs X_1, X_2, X_3, X_4, X_5, et, par suite, V ne peut avoir d'autres valeurs que celles qui sont racines de l'équation

$$Y = X_1 X_2 X_3 X_4 X_5 = 0,$$

puisque le premier membre est une fonction symétrique de b, c, d, e, f. Il s'ensuit que Y est divisible par le produit

$$Z = (x - V_1)(x - V_2)(x - V_3)(x - V_4)(x - V_5)(x - V_6).$$

Le même raisonnement prouve que V ne peut avoir d'autres valeurs que celles qui sont racines de l'équation $\frac{Y}{Z} = 0$, puis d'autres valeurs que celles qui sont racines de l'équation $\frac{Y}{Z^2} = 0$, ce qui est impossible; car cette dernière équation est seulement du troisième degré et n'a que trois racines. Il est donc établi que 3 ne peut être le nombre des valeurs que prend V par les permutations des quatre lettres c, d, e, f.

Donc la fonction V prend ses 6 valeurs par les permutations de quatre lettres quelconques c, d, e, f. Il en résulte, d'après le lemme VI, que V ne peut pas être symétrique par rapport à deux lettres a et b.

3°. Le nombre des valeurs que prend V par les permutations de trois lettres quelconques

$$d, \; e, \; f,$$

est 1, 2, 3 ou 6, car il doit diviser le produit 1.2.3. Si ce

nombre était 1, la fonction V aurait 1 ou 4 valeurs par les permutations de c, d, e, f, ce qui n'a pas lieu; s'il était 2, la fonction V aurait 2 ou 8 valeurs par les permutations des mêmes quatre lettres (vingtième leçon), ce qui n'a pas lieu non plus. Enfin, si le même nombre était 3, la fonction V serait symétrique par rapport à deux lettres, ce qui est impossible, comme on l'a vu plus haut.

Donc la fonction V prend ses 6 valeurs par les seules permutations de trois lettres quelconques d, e, f; ce qui démontre la proposition énoncée.

Je dis maintenant que :

Les quinze transpositions que l'on peut former avec les six lettres de la fonction V sont équivalentes trois à trois.

D'après ce qui précède, les 6 valeurs de V correspondent aux six arrangements

abcdef, *abcdfe*, *abcefd*, *abcfed*, *abcfde*, *abcedf*.

Si l'on transpose la lettre c avec l'une quelconque des lettres d, e, f, on obtiendra six nouveaux arrangements qui correspondront encore aux 6 valeurs distinctes de V. D'où il suit que parmi les vingt-quatre arrangements que l'on déduit de

abcdef,

en faisant les vingt-quatre permutations des lettres c, d, e, f, il y en a nécessairement quatre qui correspondent à la même valeur de V. Or, deux arrangements où trois des six lettres occupent les mêmes places ne peuvent correspondre à la même valeur de V, puisque cette fonction prend toutes ses valeurs par les seules permutations de trois lettres; donc les trois arrangements qui font acquérir à V la même valeur que l'arrangement

(1) *abcdef*

sont compris dans les neuf suivants :

(A)	(2)	*abdcfe*,	(3)	*abefcd*,	(4)	*abfedc*,
	(5)	*abfecd*,	(6)	*abdefc*,	(7)	*abecfd*,
	(8)	*abefdc*,	(9)	*abfcde*,	(10)	*abdfec*.

Or, les six arrangements (5), (6), (7), (8), (9), (10) peuvent se déduire de (1) par une substitution circulaire des quatre lettres *c*, *d*, *e*, *f*. Il arrivera donc de deux choses l'une : ou bien la fonction V ne sera pas changée par une certaine substitution circulaire des quatre lettres *c*, *d*, *e*, *f*, ou bien les arrangements (1), (2), (3), (4) donneront à V la même valeur. Si le dernier cas a lieu, on voit que V ne change pas par la transposition de deux quelconques des quatre lettres *c*, *d*, *e*, *f*, pourvu qu'on transpose en même temps les deux autres. En d'autres termes, la transposition de deux des quatre lettres *c*, *d*, *e*, *f* équivaut à la transposition des deux autres; car si la transposition (*c*, *d*) change V en V_1, la transposition (*e*, *f*) changera V_1 en V; par suite, elle changerait V en V_1, puisqu'en faisant deux fois de suite la même transposition on ne fait aucun changement. Si, au contraire, les arrangements (1), (2), (3), (4) ne donnent pas à V la même valeur, cette fonction sera invariable par une certaine substitution circulaire des quatre lettres *c*, *d*, *e*, *f*, et, par suite, elle ne changera pas non plus en répétant deux ou trois fois cette même substitution. Il s'ensuit que les trois arrangements parmi les neuf considérés, qui donnent à V la même valeur que l'arrangement (1), sont compris dans l'une des lignes horizontales suivantes :

(B)	(5) *abfecd*,	(2) *abdcfe*,	(8) *abcfde*,
	(6) *abdefc*,	(3) *abcfed*,	(9) *abfcde*,
	(7) *abecfd*,	(4) *abfedc*,	(10) *abdfce*.

On voit que l'un des arrangements (2), (3), (4) donne à V la même valeur que l'arrangement (1). Or, on passe de l'arrangement (1) à l'un de ces trois-ci par la transposition de deux des quatre lettres *c*, *d*, *e*, *f* exécutée simultanément avec la transposition des deux autres. Donc il y a, dans tous les cas, deux lettres parmi les quatre *c*, *d*, *e*, *f*, dont la transposition équivaut à la transposition des deux autres.

Nous supposerons que, dans la valeur de V,

$$V = \varphi(a, b, c, d, e, f),$$

de laquelle on part, pour former toutes les autres, par les sub-

stitutions, les places occupées par les lettres

$$a,\ b,\ c,\ d,\ e,\ f,$$

soient représentées respectivement par

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,$$

et nous introduirons ces nombres au lieu des lettres dans les substitutions. Ainsi, par exemple, la transposition des lettres qui occupent les rangs 1 et 2 sera représentée par $(1,\ 2)$.

D'après ce qui précède, la transposition de deux des quatre dernières lettres de V équivaut à la transposition des deux autres. On peut supposer que ces deux transpositions équivalentes soient $(3,\ 4)$ et $(5,\ 6)$; car il est permis de changer les noms des lettres de V. On aura donc

$$(3,\ 4) = (5,\ 6)$$

Considérons les lettres qui occupent les rangs 2, 4, 5, 6; la transposition de deux de ces quatre lettres sera équivalente à la transposition des deux autres. Or, on ne peut avoir $(2,\ 4) = (5,\ 6)$, car il en résulterait $(2,\ 4) = (3,\ 4)$, et je dis que cela est impossible. En effet, deux transpositions qui ont une lettre commune équivalent à une permutation circulaire de trois lettres (dix-neuvième leçon); or notre fonction V change par une permutation circulaire de trois lettres, elle changera donc aussi par les transpositions simultanées $(2,\ 4)$ et $(3,\ 4)$, et, par suite, ces transpositions ne peuvent être équivalentes. On a donc $(2,\ 5) = (4,\ 6)$ ou $(2,\ 6) = (4,\ 5)$. On peut supposer

$$(2,\ 5) = (4,\ 6);$$

car, jusqu'ici, rien ne distingue l'une de l'autre les lettres qui occupent les rangs 3 et 4 ou 5 et 6.

Si l'on considère ensuite les lettres qui occupent les rangs 2, 3, 5, 6, puis celles qui occupent les rangs 2, 3, 4, 6, puis enfin celles qui occupent les rangs 2, 3, 4, 5, et qu'on se rappelle que deux transpositions qui ont une lettre commune ne

peuvent être équivalentes, on trouvera

$$(2, 6) = (3, 5),$$
$$(2, 4) = (3, 6),$$
$$(2, 3) = (4, 5).$$

D'où il suit que les dix transpositions que l'on peut faire avec cinq quelconques des six lettres a, b, c, d, e, f, sont deux à deux équivalentes. D'après cela, si l'on considère les quinze transpositions que l'on peut faire avec les six lettres, il est évident que chacune des cinq qui contiennent la première lettre sera équivalente à deux des dix autres, et comme deux transpositions qui ont une lettre commune ne peuvent être égales, on aura nécessairement

$$(1, 2) = (3, 4) = (5, 6),$$
$$(1, 3) = (2, 5) = (4, 6),$$
$$(1, 4) = (2, 6) = (3, 5),$$
$$(1, 5) = (2, 4) = (3, 6),$$
$$(1, 6) = (2, 3) = (4, 5),$$

ce qui démontre la proposition énoncée. Je dis enfin que :

On peut former trois substitutions circulaires de quatre, de cinq et de six lettres respectivement, qui laissent la fonction V invariable.

En effet, on voit, par ce qui précède, qu'il est impossible que les six transpositions que l'on peut faire avec quatre lettres seulement, soient deux à deux équivalentes; car il en résulterait l'égalité impossible de deux transpositions ayant une lettre commune. Donc, à cause de l'hypothèse admise $(3, 4) = (5, 6)$, les trois arrangements du tableau (A) ou (B) qui donnent à V la même valeur que

abcdef,

sont

abfecd, *abdcfe*, *abcfde*.

On conclut de là que la fonction V est invariable par la substitution circulaire

$$(3) \qquad \begin{pmatrix} 3 & 6 & 4 & 5 \\ 6 & 4 & 5 & 3 \end{pmatrix};$$

La fonction V étant invariable par les transpositions simultanées (3, 4) et (5, 6), on a

$$V = \varphi(a, b, c, d, e, f) = \varphi(a, b, d, c, f, e);$$

faisant encore les transpositions équivalentes (2, 4), (3, 6), il vient

$$V = \varphi(a, b, c, d, e, f) = \varphi(a, b, d, c, f, e)$$
$$= \varphi(a, c, e, b, f, d);$$

donc la fonction V n'est pas changée par la substitution circulaire

$$(4) \qquad \begin{pmatrix} 2, & 3, & 5, & 6, & 4 \\ 3, & 5, & 6, & 4, & 2 \end{pmatrix}.$$

Si l'on applique la substitution (4) à la fonction

$$V = \varphi(a, b, c, d, e, f),$$

il vient

$$V = \varphi(a, c, e, b, f, d);$$

faisant maintenant la substitution (3), il vient

$$V = \varphi(a, c, d, f, e, b);$$

faisant enfin les transpositions équivalentes (1, 6) et (4, 5), on obtient

$$V = \varphi(b, c, d, e, f, a):$$

d'où il suit que la fonction V n'est pas changée par la substitution circulaire

$$(5) \qquad \begin{pmatrix} 1, & 2, & 3, & 4, & 5, & 6 \\ 2, & 3, & 4, & 5, & 6, & 1 \end{pmatrix}.$$

On voit donc que les fonctions de six lettres qui ont 6 valeurs et qui ne sont pas symétriques par rapport à cinq lettres, restent invariables par trois substitutions circulaires, l'une de quatre lettres; la deuxième de cinq lettres et la troisième de six lettres; ce qu'il fallait démontrer.

Nous pouvons maintenant conclure la composition des fonctions V que nous considérons. En effet, il est évident qu'on peut passer d'un arrangement des six lettres a, b, c, d, e, f, un autre arrangement quelconque, en exécutant une ou plusieurs fois sur les lettres du premier arrangement, une ou

plusieurs des cinq substitutions circulaires,

$$\begin{pmatrix}5, & 6\\ 6, & 5\end{pmatrix}, \quad \begin{pmatrix}4, & 5, & 6\\ 5, & 6, & 4\end{pmatrix},$$

$$\begin{pmatrix}3, & 6, & 4, & 5\\ 6, & 4, & 5, & 3\end{pmatrix}, \begin{pmatrix}2, & 3, & 5, & 6, & 4\\ 3, & 5, & 6, & 4, & 2\end{pmatrix}, \begin{pmatrix}1, & 2, & 3, & 4, & 5, & 6\\ 2, & 3, & 4, & 5, & 6, & 1\end{pmatrix},$$

dont les deux premières seules changent nos fonctions V. Il s'ensuit que toutes ces fonctions changent ou restent invariables par les mêmes substitutions; elles sont donc semblables, et, par suite, elles peuvent s'exprimer rationnellement en fonction de l'une quelconque d'entre elles et de fonctions symétriques. Il suffit, d'après cela, d'indiquer la formation d'un type.

Formons les produits deux à deux des six lettres a, b, c, d, e, f et faisons les sommes des trois produits correspondants aux transpositions équivalentes écrites plus haut. On aura les cinq fonctions suivantes :

$$\begin{aligned} &ab + cd + ef,\\ &ac + be + df,\\ &ad + bf + ce,\\ &ae + bd + cf,\\ &af + bc + de. \end{aligned}$$

Si l'on applique à ces cinq fonctions l'une quelconque des substitutions circulaires

$$\begin{pmatrix}abcdef\\ bcdefa\end{pmatrix}, \quad \begin{pmatrix}bcefd\\ cefdb\end{pmatrix}, \quad \begin{pmatrix}cfde\\ fdec\end{pmatrix},$$

on voit qu'elles ne font que s'échanger les unes dans les autres : donc leur produit

$$(ab + cd + ef)(ac + be + df)(ad + bf + ce)(ae + bd + cf)(af + bc + de)$$

ne changera par aucune des trois substitutions circulaires, et comme il n'est pas symétrique, il a nécessairement 6 valeurs.

NOTE IX.

SUR L'ÉQUATION $\frac{x^p - 1}{x - 1} = 0$, OU p DÉSIGNE UN NOMBRE PREMIER.

Si p est un nombre premier et que a soit une racine primitive pour ce nombre premier, les racines de l'équation

$$\frac{x^p - 1}{x - 1} = 0$$

peuvent être représentées par

$$x, \quad x^a, \quad x^{a^2}, \ldots, \quad x^{a^{p-2}}.$$

De cette seule propriété des racines résulte, comme nous l'avons vu dans la vingt-septième leçon, la possibilité de résoudre algébriquement l'équation. La méthode que M. Gauss a fait connaître dans ses *Disquisitiones arithmeticæ*, pour effectuer cette résolution, s'appuie sur la propriété qu'a l'équation

$$\frac{x^p - 1}{x - 1} = 0$$

d'être irréductible. Cette propriété importante est utile dans un grand nombre de questions; nous nous proposons de l'établir ici.

LEMME I. — *Si un polynôme* X *à coefficients entiers est décomposable en deux facteurs commensurables* X_1 *et* X_2, *de manière que l'on ait*

$$X = X_1 X_2,$$

tous les coefficients des polynômes X_1 *et* X_2 *seront entiers, ou, s'ils*

ne le sont pas, on pourra trouver deux entiers m et n tels, que tous les coefficients des polynômes $\frac{m}{n}X_1$ *et* $\frac{n}{m}X_2$ *soient entiers.*

Supposons, en effet, que les coefficients des polynômes X_1 et X_2 ne soient pas tous entiers. Réduisons les termes de chaque polynôme au même dénominateur, puis désignons par D_1, D_2 les deux dénominateurs obtenus, et par α un nombre premier quelconque; on pourra écrire

$$X_1 = \frac{P_1\alpha + Q_1}{D_1}, \quad X_2 = \frac{P_2\alpha + Q_2}{D_2},$$

$P_1\alpha$ ou $P_2\alpha$ désignant, dans le numérateur de X_1 ou X_2, la somme des termes divisibles par α, tandis que Q_1 ou Q_2 désigne la somme des termes non divisibles par α; on aura, d'après cela,

$$X = \frac{P_1P_2\alpha^2 + (P_1Q_2 + P_2Q_1)\alpha + Q_1Q_2}{D_1D_2}.$$

Supposons maintenant que α soit l'un des facteurs premiers de D_1; X étant entier, il faut que Q_1Q_2 soit divisible par α; cela exige que l'un des polynômes Q_1 et Q_2 se réduise à zéro; car, autrement, le premier terme du produit Q_1Q_2, supposé ordonné, serait divisible par α, ce qui est impossible, puisque aucun des termes de Q_1 et de Q_2 n'est divisible par α. D'ailleurs Q_1 n'est pas nul, car on peut admettre que la fraction qui représente la valeur de X_1 soit réduite à sa plus simple expression; donc il faut que Q_2 soit nul.

On peut conclure de là que si les fonctions X_1 et X_2 ne sont pas entières relativement aux coefficients, et qu'on réduise les termes de chacune de ces fonctions au même dénominateur, tout facteur premier α qui se trouve au dénominateur de l'une des fonctions se trouve au numérateur de l'autre. En supprimant ce facteur α, on obtient deux nouvelles fonctions qui ont encore pour produit X, et auxquelles on peut appliquer le même raisonnement; et ainsi de suite. Il résulte évidemment de là qu'on peut trouver deux entiers m et n tels, que tous les coef-

ficients des polynômes $\frac{m}{n}X_1$ et $\frac{n}{m}X_2$ soient entiers, et la fonction X, qui a pour valeur

$$X = \frac{m}{n}X_1 \times \frac{n}{m}X_2,$$

sera décomposée en deux facteurs ayant pour coefficients des nombres entiers.

Lemme II. — *Si dans un polynôme X de degré quelconque, le terme le plus élevé en x a pour coefficient l'unité, que tous les autres coefficients soient des entiers divisibles par un nombre premier p, et enfin que le terme indépendant de x soit égal à $\pm p$, l'équation*

$$X = 0$$

sera irréductible.

En effet, si cette équation n'est pas irréductible, on aura

$$X = \left(x^{\mu} + a_1 x^{\mu-1} + \ldots + a_{\mu-1} x + a_{\mu}\right)\left(x^{\nu} + b_1 x^{\nu-1} + \ldots + b_{\nu-1} x + b_{\nu}\right),$$

$a_1, a_2 \ldots b_1, b_2, \ldots$ étant des coefficients entiers et μ, ν étant des exposants entiers égaux ou supérieurs à 1 dont la somme $\mu + \nu$ est égale au degré de X. Le dernier terme de X étant égal à $\pm p$, on a $a_{\mu} b_{\nu} = \pm p$; en outre, comme p est premier, l'un des nombres a_{μ}, b_{ν} doit être égal à ± 1 et l'autre à $\pm p$; nous supposerons

$$a_{\mu} = \pm 1, \quad b_{\nu} = \pm p.$$

On a identiquement, par hypothèse,

$$X \equiv x^{\mu+\nu} \pmod{p},$$

ou

$$\left(x^{\mu} + \ldots + a_{\mu-1} x \pm 1\right)\left(x^{\nu} + \ldots + b_{\nu-1} x \pm p\right) \equiv x^{\mu+\nu} \pmod{p};$$

on peut supprimer le terme $\pm p$ dans le second facteur du

premier membre, et il vient alors

$$\left(x^{\mu}+\ldots+a_{\mu-1}x\pm 1\right)\left(x^{\nu}+\ldots+b_{\nu-2}x^{2}+b_{\nu-1}x\right)\equiv x^{\mu+\nu} \pmod{p}.$$

Le terme le moins élevé en x, dans le premier membre est $\pm b_{\nu-1}x$; donc il faut que $b_{\nu-1}$ soit divisible par p; on peut alors supprimer le terme $b_{\nu-1}x$ dans le second facteur du premier membre; il vient alors

$$\left(x^{\mu}+\ldots+a_{\mu-1}x\pm 1\right)\left(x^{\nu}+\ldots+b_{\nu-2}x^{2}\right)\equiv x^{\mu+\nu} \pmod{p}.$$

En continuant ce raisonnement, on voit que tous les coefficients $b_1, b_2, \ldots, b_\nu$ sont divisibles par p, et, par suite, que l'on a

$$\left(x^{\mu}\pm a_1 x^{\mu-1}+\ldots+a_{\mu-1}x\pm 1\right)x^{\nu}\equiv x^{\mu+\nu} \pmod{p}.$$

Or cela est impossible, puisque le coefficient de x^{ν} dans le premier membre est égal à ± 1; donc l'équation

$$X = 0$$

est irréductible.

Théorème. — *L'équation*

$$\frac{x^p - 1}{x - 1} = 0,$$

où p désigne un nombre premier, est irréductible.

Posons $x = z + 1$; l'équation que nous considérons devient

$$\frac{(z+1)^p - 1}{z} = 0,$$

ou

$$z^{p-1} + pz^{p-2} + \frac{p(p-1)}{1.2} z^{p-3} + \ldots + \frac{p(p-1)}{1.2} z + p = 0.$$

Cette équation en z est irréductible, d'après le lemme qui précède; donc la proposée est elle-même irréductible.

La démonstration que nous venons de donner ne suppose pas, comme on voit, la connaissance des propriétés des racines de l'équation binôme; elle est due à Eisenstein. Les deux lemmes démontrés plus haut suffisent pour établir le théorème plus général que voici :

Si p est un nombre premier et que μ soit un entier quelconque, l'équation

$$f(x) = \frac{x^{p^\mu} - 1}{x^{p^{\mu-1}} - 1} = 0$$

est irréductible.

En effet, posons $x = z + 1$, on aura

$$x^p \equiv z^p + 1,\ x^{p^2} \equiv z^{p^2} + 1, \ldots, x^{p^{\mu-1}} \equiv z^{p^{\mu-1}} + 1 \pmod{p};$$

d'où

$$f(z+1) \equiv z^{p^{\mu-1}(p-1)} \pmod{p}.$$

On a d'ailleurs, pour $x = 1$,

$$f(1) = p;$$

donc, d'après le lemme II, l'équation $f(z+1) = 0$ est irréductible; par suite, la proposee $f(x) = 0$ est elle-même irréductible.

Remarque. — M. Léopold Kronecker a publié, dans le tome XXIX du Journal de M. Crelle, une démonstration très-élégante pour établir l'irréductibilite de l'équation

$$\frac{x^p - 1}{x - 1} = 0,$$

quand p est un nombre premier. J'ai montré depuis (*Journal de Mathématiques pures et appliquées*, tome XV) que le raisonnement de M. Kronecker suffit, avec quelques modifications, pour établir l'irréductibilité de l'équation plus générale

$$\frac{x^{p^\mu} - 1}{x^{p^{\mu-1}} - 1} = 0.$$

Dans un Mémoire qui n'est pas encore publié, M. Kronecker vient de prouver généralement, à l'aide de principes nouveaux, que l'équation binôme

$$x^m - 1 = 0$$

devient irréductible, quel que soit m, quand on l'a débarrassée de ses racines non primitives.

J'avais énoncé ce théorème, sans le démontrer, dans l'article auquel je viens de faire allusion.

NOTE X.

SUR UNE PROPRIÉTÉ REMARQUABLE DE LA FONCTION $\dfrac{x^p-1}{x-1}$, OÙ p DÉSIGNE UN NOMBRE PREMIER.

Soit p un nombre premier, et posons

$$X=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+x+1.$$

Désignons par a une racine primitive pour le nombre premier p, et par r une racine de l'équation

$$(1)\qquad X=0;$$

les racines de l'équation (1) seront

$$r^a,\ r^{a^2},\ r^{a^3},\ldots,\ r^{a^{p-1}},$$

et l'on aura

$$a^{p-1}\equiv 1\pmod{p}\quad\text{et}\quad r^{a^{p-1}}=r.$$

Si l'on fait

$$y_1=r^{a^2}+r^{a^4}+r^{a^6}+\ldots+r^{a^{p-1}},$$
$$y_2=r^a+r^{a^3}+r^{a^5}+\ldots+r^{a^{p-2}},$$

les quantités y_1 et y_2 (vingt-sixième leçon) seront les racines d'une équation du second degré à coefficients commensurables, et l'équation (1) se décomposera en deux autres, chacune du degré $\dfrac{p-1}{2}$, et dont les coefficients seront des fonctions rationnelles de y_1 ou de y_2. Nous nous proposons, dans cette Note, d'étudier les détails de la décomposition dont il s'agit.

Occupons-nous, en premier lieu, de former l'équation en y,

qui a pour racines y_1 et y_2. On a d'abord

(2) $$y_1 + y_2 = -1,$$

car $y_1 + y_2$ exprime la somme de toutes les racines de l'équation (1). Ensuite, comme y_1 et y_2 ne changent pas, quand on change r en r^a ou en r^{a^2} on etc., on a

$$y_1^2 + y_2^2 = \frac{1}{\left(\frac{p-1}{2}\right)} \sum \left(x^{a^2} + x^{a^4} + x^{a^6} + \ldots + x^{a^{p-1}}\right)^2,$$

le signe $\sum$ s'étendant à toutes les racines x de l'équation (1).

Or on a

$$\left(x^{a^2} + x^{a^4} + \ldots + x^{a^{p-1}}\right)^2 = \sum x^{a^{2m} + a^{2n}},$$

le signe $\sum$ s'étendant ici à toutes les valeurs 1, 2, 3, ..., $\frac{p-1}{2}$ des entiers m et n; si donc on désigne par $S(\mu)$ la somme des puissances $\mu^{\text{ièmes}}$ des racines de l'équation (1), on aura

$$y_1^2 + y_2^2 = \frac{1}{\left(\frac{p-1}{2}\right)} \sum S(a^{2m} + a^{2n});$$

le signe $\sum$ s'étend à toutes les valeurs 1, 2, 3, ..., $\frac{p-1}{2}$ des entiers m et n, et il embrasse, par suite, $\left(\frac{p-1}{2}\right)^2$ termes. Comme a est une racine primitive de p, on a

$$a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p},$$

et il ne saurait y avoir aucune puissance de a d'un degré inférieur à $\frac{p-1}{2}$ congrue à -1 suivant le module p. D'après cela, si p

est de la forme $4i+1$, la somme

$$a^{2m}+a^{2n}$$

ne sera divisible par p que pour les $2i=\frac{p-1}{2}$ systèmes suivants de valeurs simultanées de m et n :

$$\begin{array}{llllllll} m= 1, & 2, & 3,\ldots, & i, & i+1, & i+2,\ldots, & 2i, \\ n=i+1, & i+2, & i+3,\ldots, & 2i, & 1, & 2,\ldots, & i; \end{array}$$

si, au contraire, p est de la forme $4i+3$, aucune des valeurs que prend la somme

$$a^{2m}+a^{2n}$$

n'est divisible par p.

Or $S(\mu)$ est égale à $p-1$ ou à -1 (treizième leçon) suivant que μ est divisible ou non divisible par p; donc, si p a la forme $4i+1$, la quantité

$$\sum S(a^{2m}+a^{2n})$$

sera égale à

$$\frac{p-1}{2}\cdot(p-1)-\left[\left(\frac{p-1}{2}\right)^2-\left(\frac{p-1}{2}\right)\right];$$

si, au contraire, p a la forme $4i+3$, la même quantité sera égale à

$$-\left(\frac{p-1}{2}\right)^2.$$

On a ainsi

$$y_1^2+y_2^2=\frac{1+p(-1)^{\frac{p-1}{2}}}{2}. \tag{3}$$

Des équations (2) et (3), on tire

$$y_1 y_2=\frac{1-p(-1)^{\frac{p-1}{2}}}{4}. \tag{4}$$

D'après cela, l'équation qui a pour racines y_1 et y_2 est

$$(5)\qquad y^2 + y + \frac{1 - p(-1)^{\frac{p-1}{2}}}{4} = 0,$$

ou

$$(2y+1)^2 - p(-1)^{\frac{p-1}{2}} = 0.$$

Considérons maintenant l'équation qui a pour racines les $\frac{p-1}{2}$ racines de l'équation (1) dont y_1 désigne la somme. Soit

$$(6)\qquad \begin{cases} X_1 = x^{\frac{p-1}{2}} - y_1 x^{\frac{p-1}{2}-1} + A_2 x^{\frac{p-1}{2}-2} + \ldots \\ \quad + A_k x^{\frac{p-1}{2}-k} + \ldots = 0 \end{cases}$$

cette équation. D'après ce qui a été dit dans la vingt-sixième leçon, les coefficients A_2, A_3, etc., peuvent s'exprimer par des fonctions rationnelles de y_1; de plus, ces fonctions peuvent être rendues linéaires (troisième leçon), puisque y_1 est racine d'une équation du second degré. Ainsi le coefficient A_k aura la forme

$$A_k = m_k + n_k y_1,$$

m_k et n_k étant des nombres rationnels; mais il est aisé de prouver, en outre, que ces nombres sont entiers. En effet, A_k est, au signe près, la somme des produits k à k des $\frac{p-1}{2}$ racines r^{a^2}, r^{a^4}, ...; chacun de ces produits est une puissance de r, et, par suite, il se réduit à l'unité ou à l'une des racines de l'équation (1). On a donc

$$A_k = \alpha_0 + \alpha_1 r + \alpha_2 r^a + \alpha_3 r^{a^2} + \alpha_4 r^{a^3} + \ldots + \alpha_{p-1} r^{a^{p-2}},$$

α_0, α_1, etc., étant des nombres entiers. Cette valeur de A_k ne changera pas si l'on change r en r^{a^2}, et, par suite, on aura

$$A_k = \alpha_0 + \alpha_1 r^{a^2} + \alpha_2 r^{a^3} + \alpha_3 r^{a^4} + \alpha_4 r^{a^5} + \ldots + \alpha_{p-1} r^{a}.$$

Je dis que les coefficients des mêmes puissances de r sont égaux dans ces deux valeurs de A_k. Supposons, en effet, que cela n'ait pas lieu ; si l'on égale les deux valeurs de A_k et qu'on rabaisse les exposants de r au-dessous de p, en faisant usage de l'équation $r^p = 1$, on aura une équation du degré $p - 1$ en r qui sera évidemment satisfaite par $r = 1$; on pourra enlever cette racine 1, et alors on voit que r sera une racine d'une équation du degré $p - 2$ à coefficients commensurables, ce qui est impossible, puisque l'équation (1) est irréductible. On a donc

$$\alpha_1 = \alpha_3 = \alpha_5 = \ldots = \alpha_{p-2},$$
$$\alpha_2 = \alpha_4 = \alpha_6 = \ldots = \alpha_{p-1},$$

et, par suite,

$$A_k = \alpha_0 + \alpha_1 y_1 + \alpha_2 y_2.$$

Enfin, chassant y_2 à l'aide de l'équation (2), la valeur de A_k prend la forme

$$A_k = m_k + n_k y_1,$$

où m_k et n_k désignent des nombres entiers positifs ou négatifs.

Le produit des racines de l'équation (6), savoir $r^{a^2 + a^4 + \ldots + a^{p-1}}$ est égal à 1, en exceptant le cas de $p = 3$; car, a étant une racine primitive de p, l'exposant $a^2 + a^4 + \ldots + n^{p-1} = \frac{a^2(a^{p-1} - 1)}{a^2 - 1}$ est divisible par p ; on a donc

$$A_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Comparons maintenant les coefficients A_k et $A_{k'}$ de deux termes également distants des extrêmes, dans X_1 ; on a la relation $k + k' = \frac{p-1}{2}$ entre les indices k et k'. La quantité $(-1)^k A_k$ est une somme de puissances de r, et la somme des inverses des mêmes puissances est égale à $(-1)^{k'} A_{k'}$; car le produit de toutes les racines de l'équation (6) est égal à 1. Cela posé, si $p = 4i + 1$, les suites

$$r^a,\ r^{a^3},\ \ldots,\ r^{a^{p-2}},$$
$$r^{a^2},\ r^{a^4},\ \ldots,\ r^{a^{p-1}}$$

restent les mêmes quand on change r en $\frac{1}{r}$; donc on a, dans ce cas,

$$A_{k'} = A_k = m_k + n_k y_1.$$

Si $p = 4i + 3$, les suites

$$r^a,\ r^{a^3},\ldots,\ r^{a^{p-2}},$$
$$r^{a^2},\ r^{a^4},\ldots,\ r^{a^{p-1}}$$

se changent l'une en l'autre quand on change r en $\frac{1}{r}$; d'ailleurs k et k' sont de parités différentes; donc l'équation $A_k = m_k + n_k y_1$ entraîne $-A_{k'} = m_k + n_k y_2 = m_k - n_k(1 + y_1)$; et l'on a, dans ce cas,

$$A_{k'} = (n_k - m_k) + n_k y_1.$$

Il résulte de là que le polynôme X_1 peut se mettre sous la forme suivante,

$$X_1 = P + Q y_1,$$

P et Q étant des polynômes à coefficients entiers qui ont respectivement pour degrés $\frac{p-1}{2}$ et $\frac{p-3}{2}$. En outre, Q est un polynôme divisible par x dans lequel les termes également distants des extrêmes sont égaux et de même signe; le polynôme P jouit de cette dernière propriété dans le cas de $p = 4i + 1$ seulement, et, par suite, il en est de même de la fonction $2P - Q$. Dans le cas de $p = 4i + 3$, la fonction $2P - Q$ a cette propriété, que les coefficients des termes également distants des extrêmes sont égaux et de signes contraires. En effet, les coefficients de $x^{\frac{p-1}{2}-k}$ et de x^k dans la fonction $2P - Q$ sont alors

$$2m_k - n_k \quad \text{et} \quad -2m_k + n_k.$$

Voici un moyen très-simple d'obtenir les valeurs des coefficients A_2, A_3, etc., de X_1. Soit λ l'un des nombres

$$1,\ 2,\ 3,\ldots\ (p-1),$$

et h un exposant entier, tel que

$$a^h \equiv \lambda \pmod{p};$$

désignons enfin par S_λ la somme des puissances $\lambda^{\text{ièmes}}$ des racines de l'équation $X_1 = 0$, on aura

$$S_\lambda = r^{a^{h+2}} + r^{a^{h+4}} + \ldots + r^{a^{h+p-1}},$$

d'où il suit que S_λ sera égale à y_1 si h est pair, c'est-à-dire si λ est résidu quadratique de p. Au contraire, S_λ sera égal à y_2 ou à $-1-y_1$ si h est impair, c'est-à-dire si λ est non-résidu quadratique de p. Connaissant ainsi les sommes de puissances semblables des racines de l'équation (6), on calculera les coefficients A_1, A_2, etc., au moyen des formules

$$S_1 - y_1 = 0,$$
$$S_2 - y_1 S_1 + 2A_2 = 0,$$
$$S_3 - y_1 S_2 + 2A_2 S_1 + 3A_3 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

On pourra exprimer ainsi A_k par une fonction entière de y_1 qu'on pourra ensuite rendre linéaire au moyen de l'équation (5).

Je passe maintenant à la démonstration d'un théorème remarquable qui est l'objet principal de cette Note.

Reprenons l'équation

$$X_1 = P + Q y_1,$$

que nous avons trouvée plus haut; en changeant y_1 en y_2, on aura

$$X_2 = P + Q y_2;$$

on a d'ailleurs $X = X_1 X_2$, donc

$$X = P^2 + PQ(y_1 + y_2) + Q^2 y_1 y_2;$$

ou, à cause de $y_1 + y_2 = -1$, $y_1 y_2 = \dfrac{1 - p(-1)^{\frac{p-1}{2}}}{4}$,

$$4X = (2P - Q)^2 - (-1)^{\frac{p-1}{2}} p Q^2.$$

Et d'après les remarques faites précédemment, on a ce théorème :

THÉORÈME. — *p étant un nombre premier et X désignant le polynôme $x^{p-1} + x^{p-2} + \ldots + x + 1$, on aura $4X = Y^2 - pZ^2$ si $p = 4i + 1$, et $4X = Y^2 + pZ^2$ si $p = 4i + 3$. Z est, dans les deux cas, un polynôme du degré $\frac{p-3}{2}$ à coefficients entiers dans lequel les termes également distants des extrêmes ont le même coefficient; Y est un polynôme du degré $\frac{p-1}{2}$ à coefficients entiers dont les termes également distants des extrêmes ont des coefficients égaux et de même signe, ou égaux et de signes contraires, suivant que $p = 4i + 1$ ou $= 4i + 3$.*

REMARQUE. — Le nombre 3 échappe à notre analyse, ainsi que nous en avons fait plus haut la remarque. L'équation

$$4(x^2 + x + 1) = Y^2 + 3Z^2$$

admet toutefois les trois solutions

$$\begin{aligned} Y &= 2x + 1, & Z &= 1, \\ Y &= x + 2, & Z &= x, \\ Y &= x - 1, & Z &= x + 1; \end{aligned}$$

mais les polynômes Y et Z relatifs à l'une quelconque de ces trois solutions ne satisfont pas à toutes les conditions indiquées dans l'énoncé du théorème précédent.

Considérons maintenant l'équation indéterminée

$$Y^2 \pm pZ^2 = 4X,$$

où l'on prend le signe + ou le signe — dans le premier membre, suivant que le nombre premier p a la forme $4i + 3$ ou la forme $4i + 1$, et cherchons si cette équation peut admettre des solutions *entières* (Y, Z) différentes de la solution à laquelle nous avons été conduit, et que nous désignerons par (Y_0, Z_0). On aura

$$\begin{aligned} &(Y + Z\sqrt{\pm p})(Y - Z\sqrt{\pm p}) \\ &= (Y_0 + Z_0\sqrt{\pm p})(Y_0 - Z_0\sqrt{\pm p}); \end{aligned}$$

il est aisé de voir que les deux équations

$$Y + Z\sqrt{\pm p} = 0, \quad Y_0 + Z_0\sqrt{\pm p} = 0,$$

qui sont chacune du degré $\frac{p-1}{2}$, ont les mêmes racines ou qu'elles n'ont aucune racine commune. En effet, si ces équations avaient n racines communes, n étant $< \frac{p-1}{2}$, on pourrait former une équation du degré n qui aurait ces n racines, et dont les coefficients ne contiendraient que la seule irrationnelle $\sqrt{\pm p}$; en isolant dans un membre les termes affectés de $\sqrt{\pm p}$ et élevant ensuite au carré, on obtiendrait une équation du degré $2n$ à coefficients rationnels et dont les racines appartiendraient à l'équation $X = 0$. Or cela est impossible, puisque cette dernière équation est irréductible. Il suit de là que la fonction $Y + Z\sqrt{\pm p}$ est divisible algébriquement par l'une des fonctions $Y_0 + Z_0\sqrt{\pm p}$, $Y_0 - Z_0\sqrt{\pm p}$; et comme on peut changer, si l'on veut, le signe de Z_0, on peut admettre que les fonctions

$$\frac{Y + Z\sqrt{\pm p}}{Y_0 + Z_0\sqrt{\pm p}}, \quad \frac{Y - Z\sqrt{\pm p}}{Y_0 - Z_0\sqrt{\pm p}}$$

sont indépendantes de x. Or, pour $x = 0$, nous avons vu que Z_0 est nul; par suite, Y_0 se réduit à ± 2. Il n'y a pas d'exception pour le cas de $p = 3$, car on peut prendre alors

$$Y_0 = x + 2 \quad \text{et} \quad Z_0 = x,$$

comme nous l'avons vu plus haut. D'après cela, on aura

$$Y + Z\sqrt{\pm p} = \frac{t + u\sqrt{\pm p}}{2}(Y_0 + Z_0\sqrt{\pm p}),$$

$$Y - Z\sqrt{\pm p} = \frac{t - u\sqrt{\pm p}}{2}(Y_0 - Z_0\sqrt{\pm p}),$$

t et u désignant les nombres entiers positifs ou négatifs, auxquels se réduisent Y et Z pour $x = 0$. En multipliant les équa-

tions précédentes entre elles, il vient

$$t^2 \mp pu^2 = 4.$$

Si l'on suppose que t et u soient des entiers quelconques satisfaisant à cette équation, les solutions de la proposée seront toutes données par les formules précédentes, d'où l'on tire

$$Y = \frac{tY_0 \pm puZ_0}{2}, \quad Z = \frac{uY_0 + tZ_0}{2}.$$

Or nous avons fait

$$Y_0 = 2P - Q, \quad Z_0 = Q,$$

P et Q étant des polynômes à coefficients entiers; on peut donc écrire

$$Y = tP + \frac{-t \pm pu}{2}Q, \quad Z = uP + \frac{t-u}{2}Q,$$

et ces valeurs de Y et Z sont entières; car, à cause de

$$t^2 \mp pu^2 = 4,$$

les nombres $-t \pm pu$ et $t - u$ sont divisibles par 2.

Supposons, en premier lieu, que p soit de la forme $4i + 3$; l'équation

$$t^2 + pu^2 = 4$$

n'admet que la solution

$$t = \pm 2, \quad u = 0,$$

sauf le cas de $p = 3$. Les formules écrites plus haut donnent alors

$$Y = \pm Y_0, \quad Z = \pm Z_0;$$

dans le cas de $p = 3$, l'équation en t et u admet en outre la solution

$$t = \pm 1, \quad u = \pm 1.$$

On peut conclure de là que l'équation proposée

$$Y^2 + pZ^2 = 4X,$$

où $p = 4i + 3$, n'admet que la seule solution (Y_0, Z_0), sauf le

cas de $p = 3$, dans lequel l'équation admet les trois solutions indiquées plus haut.

Supposons, en second lieu, que p soit de la forme $4i+1$; l'équation

$$t^2 - pu^2 = 4$$

admet une infinité de solutions, et, par conséquent, l'équation proposée

$$Y^2 - pZ^2 = 4X$$

admettra aussi une infinité de solutions distinctes qui seront données par les formules écrites plus haut.

Les résultats que nous venons de trouver relativement à la fonction $\frac{x^p - 1}{x - 1}$, peuvent s'étendre à la fonction plus générale $\frac{x^p - y^p}{x - y}$, qu'on déduit de la première en changeant x en $\frac{x}{y}$, et en multipliant ensuite par y^{p-1}. On peut évidemment, d'après cela, énoncer le théorème suivant :

Théorème. — *p étant un nombre premier, on peut satisfaire à l'équation*

$$Y^2 - (-1)^{\frac{p-1}{2}} p Z^2 = 4\frac{x^p - y^p}{x - y},$$

en prenant pour Y et Z des fonctions entières de x et y. En outre, cette équation a une infinité de solutions si $p = 4i+1$; elle en a trois si $p = 3$, et une seule si p est un nombre premier $4i+3$ plus grand que 3.

NOTE XI.

SUR LA LOI DE RÉCIPROCITÉ QUI EXISTE ENTRE DEUX NOMBRES PREMIERS QUELCONQUES.

Pour donner une idée de l'importance des résultats que nous avons obtenus dans la Note précédente, nous allons montrer comment on peut en déduire la *loi de réciprocité* qui existe entre deux nombres premiers quelconques et qui a été découverte par l'illustre Legendre (*). On connaît aujourd'hui un grand nombre de démonstrations de cette loi de réciprocité ; la plus simple est, sans contredit, celle que Legendre a donnée, d'après Jacobi, dans le second volume de sa *Théorie des Nombres*, et que nous allons reproduire ici.

On sait, par le théorème de Fermat, que si N est un entier quelconque, et p un nombre premier qui ne divise pas N, le nombre $N^{p-1} - 1$ est divisible par p ; or ce nombre est le produit des deux facteurs $N^{\frac{p-1}{2}} - 1$ et $N^{\frac{p-1}{2}} + 1$: il faut donc que l'un de ces facteurs soit divisible par p ; par conséquent, le reste de la division de $N^{\frac{p-1}{2}}$ par p sera toujours égal à $+1$ ou à -1 : Legendre désigne ce reste au moyen de la notation $\left(\frac{N}{p}\right)$. D'après ce que nous avons avons vu dans la vingt-quatrième leçon, si N est résidu quadratique de p, on a $\left(\frac{N}{p}\right) = +1$; au contraire, si N est non-résidu quadratique, on a $\left(\frac{N}{p}\right) = -1$.

Cela posé, la loi de réciprocité de Legendre consiste en ce

(*) *Voir* la *Théorie des Nombres,* troisième édition, tome I, page 230, et tome II, pages 57 et 391.

que, si p et q sont deux nombres premiers impairs quelconques, on a toujours

$$\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{q}{p}\right).$$

Pour démontrer cette égalité, considérons l'équation

$$\frac{x^p - 1}{x - 1} = 0,$$

désignons par r l'une de ses racines et par a une racine primitive pour le nombre premier p; posons

$$y_1 = r + r^{a^2} + r^{a^4} + \ldots + r^{a^{p-3}},$$
$$y_2 = r^a + r^{a^3} + r^{a^5} + \ldots + r^{a^{p-2}};$$

on aura (*voir* la Note précédente)

$$y_1 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{(-1)^{\frac{p-1}{2}} p},$$

$$y_2 = -\frac{1}{2} \mp \frac{1}{2}\sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Si donc on fait

$$P = r - r^a + r^{a^2} - r^{a^3} + \ldots + r^{a^{p-3}} - r^{a^{p-2}},$$

on aura

$$P = y_1 - y_2 = \pm\sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Soit maintenant q un nombre premier impair différent de p. Si l'on élève le polynôme P à la puissance q, le résultat contiendra d'abord les puissances $q^{\text{ièmes}}$ des différents termes de P, puis d'autres termes dont les coefficients sont tous divisibles par q (*). Si l'on désigne par $q \sum A r^{\alpha}$ l'ensemble de ces der-

(*) *Voir* la vingt-cinquième leçon (page 357).

niers termes et que l'on pose

$$Q = r^{q} - r^{qa} + r^{qa^2} - \ldots + r^{qa^{p-3}} - r^{qa^{p-2}},$$

on aura

$$P^{q} = Q + q \sum A r^{\alpha}.$$

Il convient maintenant de distinguer le cas de $\left(\frac{q}{p}\right) = +1$ et celui de $\left(\frac{q}{p}\right) = -1$.

1°. Soit $\left(\frac{q}{p}\right) = +1$. Cela veut dire que q est racine de la congruence

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p},$$

dont les racines sont

$$a^2,\ a^4,\ a^6, \ldots,\ a^{p-1};$$

on a donc nécessairement

$$q \equiv a^{2n} \pmod{p},$$

n étant un entier au plus égal à $\frac{p-1}{2}$. Par suite, la valeur de Q est

$$Q = r^{a^{2n}} - r^{a^{2n+1}} + r^{a^{2n+2}} - \ldots + r^{a^{2n+p-3}} - r^{a^{2n+p-2}},$$

et, en rabaissant les exposants de a au-dessous de $p-1$, on a évidemment

$$Q = P.$$

2°. Soit $\left(\frac{q}{p}\right) = -1$. Dans ce cas, q est racine de la congruence

$$x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p},$$

laquelle a pour racines

$$a,\ a^3,\ a^5, \ldots,\ a^{p-2}.$$

On a donc

$$q \equiv a^{2n+1} \pmod{p},$$

n étant un entier. Il vient alors

$$Q = r^{a^{2n+1}} - r^{a^{2n+2}} + r^{a^{2n+3}} - \ldots + r^{a^{2n+p-2}} - r^{a^{2n+p-1}},$$

et, en rabaissant les exposants de a au-dessous de $p-1$, on a

$$Q = -P.$$

Donc on a, dans tous les cas,

$$Q = \left(\frac{q}{p}\right) P,$$

et, par suite,

$$P^q = \left(\frac{q}{p}\right) P + q \sum A r^\alpha,$$

ou

$$P^{q-1} - \left(\frac{q}{p}\right) = q \frac{\sum A r^\alpha}{P}.$$

Substituant dans le premier membre la valeur de P, il se réduit à

$$p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} - \left(\frac{q}{p}\right),$$

quantité qui est un nombre entier. Quant au second membre $q \cdot \frac{\sum A r^\alpha}{P}$, il se réduira donc aussi à un nombre entier; la même chose peut se dire de son carré $(-1)^{\frac{p-1}{2}} \frac{q^2}{p} \left(\sum A r^\alpha\right)^2$. Il s'ensuit que le carré de $\sum A r^\alpha$ est une fonction symétrique et entière des racines de l'équation $\frac{x^p - 1}{x - 1} = 0$, et, par suite, qu'il a pour

valeur un nombre entier ; de plus, cet entier est divisible par p, puisqu'en le multipliant par $\frac{q^2}{p}$ on doit obtenir un entier. Il résulte de là que $q\,\frac{\sum A r^\alpha}{P}$ est un entier dont le carré est divisible par q ; donc ce nombre est lui-même divisible par q et l'on a

$$\frac{\sum A r^\alpha}{P} = M,$$

M étant un nombre entier. Par conséquent,

$$p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} - \left(\frac{q}{p}\right) = Mq;$$

remarquant que

$$p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) + \text{un multiple de } q,$$

et supprimant de part et d'autre les multiples de q, il vient

$$\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{q}{p}\right);$$

ce qu'il fallait démontrer.

NOTE XII.

SUR LA RÉSOLUTION ALGÉBRIQUE DE L'ÉQUATION DU NEUVIÈME DEGRÉ A LAQUELLE CONDUIT LA RECHERCHE DES POINTS D'INFLEXION DES COURBES DU TROISIÈME DEGRÉ.

M. Otto Hesse, géomètre éminent de Kœnigsberg, a publié dans le Journal de M. Crelle (tome XXVIII, page 68, et tome XXXIV, page 191), deux Mémoires remarquables sur la détermination des points d'inflexion des courbes du troisième degré. Dans son second Mémoire, M. Hesse a démontré généralement que :

Les points d'inflexion d'une courbe algébrique du degré n sont situés sur une seconde courbe du degré $3(n-2)$, et, par suite, que :

Une courbe algébrique du degré n n généralement $3n(n-2)$ *points d'inflexion, réels ou imaginaires.*

Dans les cas particuliers, quelques-uns de ces points d'inflexion peuvent être situés à l'infini. Lorsque $n=3$, on a ce théorème :

Les points d'inflexion d'une courbe du troisième degré sont situés sur une seconde courbe du troisième degré.

Et, par suite, la recherche des points d'inflexion d'une courbe du troisième degré dépend généralement de la résolution d'une equation du neuvième degré à une inconnue. Or il est très-remarquable que cette équation du neuvième degré soit toujours résoluble algébriquement, et qu'il suffise, pour effectuer cette résolution, de résoudre une seule équation du quatrième degré et plusieurs équations du troisième degré. Cette proposition se déduit facilement, comme nous le ferons voir plus loin, du théorème de M. Hesse énoncé plus haut, et d'un autre théorème démontré pour la première fois par Maclaurin dans son *Essai sur les lignes du troisième degré,* théorème qui consiste en ce que :

La droite qui joint deux points d'inflexion d'une courbe du

troisième degré, rencontre la courbe en un troisième point d'inflexion.

La démonstration que M. Hesse a donnée dans son second Mémoire, pour établir la resolubilité de l'équation du neuvième degré dont il s'agit, suppose également le théorème de Maclaurin. M. Hesse fait voir qu'il existe certaines relations entre les racines, et il démontre généralement que toute équation du neuvième degré dont les racines ont cette même propriété, est résoluble par radicaux. L'analyse de M. Hesse est assez remarquable pour que je croie devoir la reproduire ici :

Sur la recherche des points d'inflexion des courbes algébriques.

Soit U une fonction quelconque entière et homogène du $n^{ième}$ degré de deux variables x et y; $U = 0$ sera une équation quelconque du degré n si l'on prend pour inconnue $\frac{x}{y}$, et cette équation aura trois racines égales si l'on peut satisfaire en même temps aux trois équations

$$U = 0, \quad \frac{dU}{dx} = 0, \quad \frac{d^2 U}{dx^2} = 0.$$

Ces équations de condition sont respectivement des degrés n, $n - 1$, $n - 2$; mais on peut à leur place prendre trois équations du même degré $n - 2$. Elles peuvent effectivement s'écrire ainsi (*) :

$$\begin{cases} U = \dfrac{1}{n(n-1)}\left(x^2 \dfrac{d^2 U}{dx^2} + 2xy\dfrac{d^2 U}{dx\,dy} + y^2\dfrac{d^2 U}{dy^2}\right) = 0, \\ \dfrac{dU}{dx} = \dfrac{1}{n-1}\left(x\dfrac{d^2 U}{dx^2} + y\dfrac{d^2 U}{dx\,dy}\right) = 0, \\ \dfrac{d^2 U}{dx^2} = 0. \end{cases}$$

(*) Cela résulte immédiatement du théorème connu dit *des fonctions homogènes*. Soit $f(x, y)$ une fonction homogène du degré μ; en multipliant x et y par $1 + \alpha$, il vient, d'après la définition des fonctions homogènes,

$$f(x + \alpha x,\ y + \alpha y) = (1 + \alpha)^{\mu} f(x, y).$$

Developpant les deux membres par rapport à α et égalant ensuite les coef-

A cause de la troisième équation, la deuxième se réduit à $\frac{d^2U}{dxdy} = 0$, et la première devient ensuite $\frac{d^2U}{dy^2} = 0$. Donc les équations de condition relatives à l'égalité de trois racines de l'équation $U = 0$, sont les suivantes, du degré $n - 2$ chacune,

$$\frac{d^2U}{dx^2} = 0, \quad \frac{d^2U}{dxdy} = 0, \quad \frac{d^2U}{dy^2} = 0.$$

On ferait voir de même que généralement les équations de condition relatives à l'égalité de m racines de l'équation $U = 0$ sont les suivantes du degré $n - m + 1$,

$$\frac{d^{m-1}U}{dx^{m-1}} = 0, \quad \frac{d^{m-1}U}{dx^{m-2}dy} = 0, \ldots \frac{d^{m-1}U}{dxdy^{m-2}} = 0, \quad \frac{d^{m-1}U}{dy^{m-1}} = 0.$$

Soit maintenant u une fonction quelconque entière et homogène du $n^{ième}$ degré, de trois variables x, y, z. Si l'on représente par $\frac{x}{z}$ et $\frac{y}{z}$ les coordonnées rectangulaires ou obliques d'un point variable, l'équation

$$u = 0$$

représentera une courbe quelconque du $n^{ième}$ degré (*). Une droite quelconque dont l'équation est

$$z = ax + by,$$

rencontre, comme on sait, la courbe en n points; si l'on porte

---

ficients des mêmes puissances de α, il vient

$$x\frac{df}{dx} + y\frac{df}{dy} = \mu f(x, y),$$

$$x^2\frac{d^2f}{dx^2} + 2xy\frac{d^2f}{dxdy} + y^2\frac{d^2f}{dy^2} = \mu(\mu - 1)f(x, y),$$

....

....

(*) M. Hesse a eu le premier l'ingénieuse idée de représenter par $\frac{x}{z}$, $\frac{y}{z}$ les coordonnées rectilignes d'un point dans un plan, et par $\frac{x}{u}$, $\frac{y}{u}$, $\frac{z}{u}$ les coordonnées dans l'espace. De cette manière, toutes les équations sont homogènes. On se fera une idée, en lisant cette Note, des avantages considérables que présente cette notation nouvelle.

la valeur de z tirée de l'équation de la droite, dans la fonction u, celle-ci devient une fonction homogène U des deux variables x et y, et les n racines de l'équation $U=0$, où l'on considère $\frac{x}{y}$ comme l'inconnue, sont les rapports des coordonnées des points où la droite rencontre la courbe. Mais l'équation de la ligne droite contient deux constantes a et b qui s'introduisent dans l'équation $U=0$; on peut établir entre ces constantes une relation telle, que deux racines de l'équation $U=0$ deviennent égales : dans ce cas, la droite devient une tangente de la courbe. Et si l'on donne aux constantes a et b des valeurs telles, que trois racines de l'équation $U=0$ deviennent égales, la droite devient une tangente en un point d'inflexion, lequel est déterminé, comme on l'a vu plus haut, par les trois équations

$$\frac{d^2U}{dx^2}=0,\quad \frac{d^2U}{dx\,dy}=0,\quad \frac{d^2U}{dy^2}=0.$$

Mais, comme U est la valeur que prend u pour $z=ax+by$, si l'on fait, pour abréger,

$$\frac{d^2u}{dx^2}=\xi,\quad \frac{d^2u}{dy^2}=\eta,\quad \frac{d^2u}{dz^2}=\zeta,$$

$$\frac{d^2u}{dy\,dz}=\xi_1,\quad \frac{d^2u}{dx\,dz}=\eta_1,\quad \frac{d^2u}{dx\,dy}=\zeta_1,$$

les trois équations précédentes pourront s'écrire comme il suit :

$$\xi+2a\eta_1+a^2\zeta=0,$$
$$\zeta_1+a\xi_1+b\eta_1+ab\zeta=0,$$
$$\eta+2b\xi_1+b^2\zeta=0.$$

Si l'on élimine a et b entre ces équations, on obtiendra l'équation d'une courbe qui rencontre la proposée aux points d'inflexion. Pour effectuer cette élimination, résolvons la deuxième équation par rapport à a, ce qui donne

$$a=-\frac{\zeta_1+b\eta_1}{\xi_1+b\zeta},$$

et portons cette valeur de a dans la première équation, nous

obtenons

$$\xi(\xi_1 + b\zeta)^2 - 2\eta_1(\zeta_1 + b\eta_1)(\xi_1 + b\zeta) + \zeta(\zeta_1 + b\eta_1)^2 = 0,$$

ou, en ordonnant par rapport à b,

$$\xi\xi_1^2 - 2\xi_1\eta_1\zeta_1 + \zeta\zeta_1^2 + (\xi\zeta - \eta_1^2)(2b\xi_1 + b^2\zeta) = 0.$$

Si enfin on multiplie la dernière des trois équations que nous considérons par $\xi\zeta - \eta_1^2$, et qu'on en retranche ensuite l'équation que nous venons de former, il vient

$$v = \xi\eta\zeta + 2\xi_1\eta_1\zeta_1 - \xi\xi_1^2 - \eta\eta_1^2 - \zeta\zeta_1^2 = 0.$$

L'équation $v = 0$ est celle de la courbe cherchée qui rencontre la proposée $u = 0$ aux points d'inflexion. Cette équation est, comme on voit, du degré $3(n-2)$, d'où il suit qu'une courbe du $n^{ième}$ degré a généralement $3n(n-2)$ points d'inflexion. En particulier, une courbe du troisième degré a neuf points d'inflexion.

Sur les points d'inflexion des courbes du troisième degré.

Nous commencerons par établir quelques propositions générales relatives aux courbes du troisième degré sur lesquelles nous aurons à nous appuyer.

Remarquons d'abord que le système formé d'une conique et d'une droite, ou le système de trois droites, constitue une variété des lignes du troisième degré.

LEMME I. — *Deux courbes du troisième degré se coupent généralement en neuf points.*

Cette proposition se déduit immédiatement du théorème de Bezout sur le degré de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations.

Remarque. — Les points d'intersection peuvent être réels ou imaginaires.

LEMME II. — *Neuf points suffisent en général pour déterminer une courbe du troisième degré.*

Il y a effectivement dix termes dans l'équation générale des courbes du troisième degré. Le coefficient de l'un de ces termes



peut être choisi arbitrairement, et il reste alors neuf coefficients indéterminés dont on peut disposer de manière à assujettir la courbe à passer par neuf points donnés. On obtient ainsi neuf équations du premier degré entre les coefficients inconnus; en général, ces équations admettent une solution unique, et, par suite, on ne peut généralement faire passer qu'une seule courbe du troisième degré par neuf points donnés (*).

LEMME III. — *Toute courbe du troisième degré qui passe par huit des neufs points d'intersection de deux courbes du troisième degré données, passe également par le neuvième point d'intersection de ces deux courbes.*

Soient Γ et Γ_1 les deux courbes du troisième degré données. Supposons qu'on se propose de faire passer une courbe du troisième degré par les neuf points d'intersection des courbes Γ et Γ_1; les neuf équations linéaires que doivent vérifier les coefficients de l'équation de la courbe inconnue, admettront les deux solutions relatives aux courbes Γ et Γ_1 qui satisfont au problème; donc ces neuf équations sont indéterminées, et l'une quelconque d'entre elles est comprise dans les huit autres. Il suit de là que, si l'on assujettit une courbe du troisième degré Γ_2 à passer par huit des points communs aux courbes Γ et Γ_1 et que, pour achever de la déterminer, on se donne une nouvelle condition arbitraire, la courbe Γ_2 passera nécessairement par le neuvième point d'intersection des courbes Γ et Γ_1.

COROLLAIRE I. — *Si trois des neuf points d'intersection de deux courbes du troisième degré sont en ligne droite, les six autres points d'intersection sont situés sur une conique.*

En effet, la droite qui passe par les trois premiers points d'intersection des courbes données Γ et Γ_1, et la conique qui passe par cinq des six autres, forment une ligne du troisième

(*) M. Chasles a publié l'année dernière de belles recherches sur les courbes du troisième et du quatrième degré. (*Voir* les *Comptes rendus de l'Académie des Sciences*, tome XXVI, page 943, et tome XXVII, pages 272, 437 et 472.) M. Chasles fait connaître en particulier deux méthodes très-remarquables pour construire la courbe du troisième degré qui passe par neuf points donnés.



degré qui passe par le neuvième point d'intersection des courbes Γ et Γ_1 ; donc la conique passe par ce neuvième point, car une courbe du troisième degré ne peut avoir quatre points en ligne droite.

Corollaire II. — *Si six des neuf points d'intersection de deux courbes du troisième degré sont situés sur une conique, les trois autres points d'intersection sont en ligne droite.*

En effet, la conique qui passe par les six premiers points d'intersection et la droite qui passe par deux des trois autres forment une ligne du troisième degré qui passe par le neuvième point d'intersection; donc la droite passe par ce neuvième point, car une conique ne peut avoir plus de six points communs avec une courbe du troisième degré. (Théorème de Bezout sur le degré de l'équation finale.)

Corollaire III. — *Si trois des neuf points d'intersection de deux courbes du troisième degré sont en ligne droite, et que trois des six autres soient aussi en ligne droite, les trois derniers seront pareillement en ligne droite.*

Ce corollaire est évidemment un cas particulier du précédent.

Remarque. — Les propositions que nous venons d'établir conduisent à un grand nombre de conséquences curieuses; mais, pour ne pas trop nous écarter de notre sujet, nous nous bornerons à montrer comment on en déduit immédiatement le théorème connu de Pascal relatif à l'hexagone inscrit dans une conique. On sait que ce théorème consiste en ce que :

Si un hexagone est inscrit dans une conique, les points de rencontre des côtés opposés sont en ligne droite.

En effet, soient A, B, C, D, E, F les sommets de l'hexagone; soient M, N, P les points d'intersection des côtés AB et DE, BC et EF, CD et FA. Les lignes du troisième ordre formées, l'une des droites AB, CD, EF, l'autre des droites BC, DE, FA, se coupent aux neuf points A, B, C, D, E, F, M, N, P. Or les six premiers points sont sur une conique; donc, les trois autres sont en ligne droite; ce qu'il fallait démontrer.

Lemme IV. — *Si $u = 0$, $v = 0$ sont les équations en coordonnées rectilignes de deux courbes du troisième degré, l'équa-*

tion générale des courbes du troisième degré qui passent par les neuf points d'intersection des courbes données sera

$$ku + v = 0,$$

k désignant une constante indéterminée.

Soient A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9 les points d'intersection réels ou imaginaires des courbes données. Si l'on se propose de faire passer une courbe du troisième degré par ces neuf points, on aura, comme on l'a vu plus haut, neuf équations linéaires auxquelles devront satisfaire les coefficients de l'équation de la courbe inconnue et parmi lesquelles huit quelconques entraînent la neuvième; mais je dis que huit de ces neuf équations sont distinctes. Effectivement, s'il en était autrement, toute courbe du troisième degré passant par sept des points donnés, A_1, A_2, A_3, A_4, A_5, A_6 et A_7 par exemple, passerait nécessairement par les deux autres A_8 et A_9; il est aisé de démontrer que cela n'est pas. En effet, considérons les trois points A_5, A_6, A_7; il y en a nécessairement deux qui ne sont en ligne droite ni avec A_8 ni avec A_9. Supposons que A_6 et A_7 soient dans ce cas; désignons par D la droite qui passe par ces deux points, et par C la conique qui passe par les points A_1, A_2, A_3, A_4, A_5. La conique C et la droite D forment une ligne du troisième degré qui passe par les sept points A_1, A_2, A_3, A_4, A_5, A_6 et A_7. Or je dis que cette ligne du troisième degré ne peut passer par aucun des points A_8 et A_9: d'abord la droite D ne contient, par hypothèse, aucun de ces points; la conique C ne peut les contenir tous deux, car elle aurait sept points communs avec une ligne du troisième degré; elle ne peut non plus contenir l'un d'eux, car l'autre serait alors sur la droite D (lemme III, corollaire II), ce qui est contre l'hypothèse.

Il résulte de là que les équations linéaires qui ont lieu entre les coefficients de la courbe du troisième degré qui passe par les neuf points A_1, A_2, etc., donneront les valeurs de huit des coefficients inconnus exprimées en fonction linéaire du neuvième, et que, par suite, l'équation générale des courbes du troisième degré, qui passent par les points communs aux courbes $u = 0$, $v = 0$, ne peut contenir qu'une seule arbitraire. Or, quelle que

soit la constante k, il est évident que la courbe représentée par l'équation

$$ku + v = 0$$

passe par les points communs aux courbes proposées; donc cette équation est la plus générale possible.

Théorème I. — *La droite qui joint deux points d'inflexion d'une courbe du troisième degré rencontre la courbe en un troisième point d'inflexion.*

Soient A et A' deux points d'inflexion d'une courbe du troisième degré Γ, et supposons que la droite AA' rencontre la courbe Γ au troisième point A''; je dis que A'' est un point d'inflexion. En effet, menons, par le point A, une sécante quelconque qui rencontre de nouveau la courbe aux points B et C; par le point A', une seconde sécante quelconque qui rencontre de nouveau la courbe aux points B' et C'; joignons BB' et CC', qui rencontrent de nouveau la courbe aux points B'' et C'' respectivement; joignons enfin A''B''. La ligne du troisième degré formée des trois droites ABC, A'B'C' et A''B'' passe par huit des points d'intersection de la courbe Γ et de la ligne du troisième degré formée des droites AA'A'', BB'B'', CC'C'', elle passera donc par le neuvième point d'intersection C''. Et comme une courbe du troisième degré ne peut avoir quatre points en ligne droite, il faut nécessairement que les trois points A'', B'', C'' soient en ligne droite. Imaginons maintenant que les sécantes BC et B'C' tournent respectivement autour des points A et A', de manière à devenir tangentes à la courbe; comme A et A' sont deux points d'inflexion, les points B et C se confondront avec A à la limite: pareillement, B' et C' se confondront avec A'; donc les droites BB'B'' et CC'C'' coïncideront avec AA'A'', et, par suite, les trois points d'intersection de la courbe avec la sécante A''B''C'' se confondront en un seul A'', qui est ainsi un point d'inflexion.

Remarque. — Bien que ce raisonnement soit géométrique, il est évident qu'il s'applique au cas des points imaginaires comme à celui des points réels.

Théorème II. — *Le nombre des droites qui passent chacune par trois points d'inflexion d'une courbe du troisième degré, est*

égal à douze. Ces douze droites forment quatre systèmes composés chacun de trois droites, et les neuf points d'inflexion de la courbe sont trois à trois sur les trois droites de chaque système.

Si l'on joint par des droites l'un des points d'inflexion de la courbe à chacun des huit autres, il est évident que ces huit droites se réduiront à quatre distinctes, puisque la droite, qui passe par deux points d'inflexion, passe aussi par un troisième, et que, d'ailleurs, quatre points d'inflexion ne sauraient être en ligne droite. Donc, parmi les droites qui joignent les neuf points d'inflexion, trois à trois, il y en a toujours quatre qui passent par un même point. En en comptant quatre pour chaque point d'inflexion, on aura 4×9 ou 36 droites; mais alors il est clair que chaque droite se trouve prise trois fois, et, par suite, que ces trente-six droites se réduisent à douze distinctes.

Soient

$$A_1,\ A_2,\ A_3,\ A_4,\ A_5,\ A_6,\ A_7,\ A_8,\ A_9$$

les neuf points d'inflexion. On peut supposer que A_1, A_2, A_3 soient en ligne droite. Parmi les douze droites que nous considérons, il y en a trois, outre la droite $A_1A_2A_3$, qui passent par chacun des points A_1, A_2, A_3; il y a donc deux droites qui ne passent ni par A_1, ni par A_2, ni par A_3. D'après cela, on peut supposer que A_4, A_5, A_6 sont en ligne droite, et alors A_7, A_8, A_9 seront aussi en ligne droite, puisque les neuf points sont à l'intersection de deux courbes du troisième degré (lemme III, corollaire III). Nous avons ainsi un premier système de trois droites, savoir :

$$A_1A_2A_3,\quad A_4A_5A_6,\quad A_7A_8A_9,$$

qui contiennent trois à trois les neuf points d'inflexion. La droite A_2A_4 ne peut passer par l'un des points A_1, A_3, A_5, A_6, elle passe donc par l'un des points A_7, A_8, A_9, et comme jusqu'ici rien ne distingue ces trois points les uns des autres, on peut supposer que la droite A_2A_4 passe par A_7; les droites A_3A_5 et A_3A_6 ne peuvent toutes deux passer par A_7, donc l'une d'elles passe par l'un des points A_8 et A_9. On peut évidemment supposer d'après cela que A_3A_5 passe par A_8, car jusqu'ici rien ne distingue

entre eux les points A_5 et A_6 ou A_8 et A_9. Alors, d'après le lemme III (corollaire III), les points A_1, A_6, A_9 sont en ligne droite. On a ainsi ce deuxième système de trois droites renfermant trois à trois les neuf points d'inflexion, savoir :

$$A_2 A_4 A_7, \quad A_3 A_5 A_8, \quad A_1 A_6 A_9.$$

Maintenant, il est évident que les droites $A_5 A_7$, $A_6 A_8$, $A_4 A_9$ passent respectivement par A_1, A_2 et A_3; et que les droites $A_8 A_1$, $A_9 A_2$, $A_7 A_3$ passent respectivement par A_4, A_5, A_6. On a donc ces deux derniers systèmes de trois droites contenant trois à trois les neuf points d'inflexion, savoir :

$$A_5 A_7 A_1, \quad A_6 A_8 A_2, \quad A_4 A_9 A_3;$$
$$A_8 A_1 A_4, \quad A_9 A_2 A_5, \quad A_7 A_3 A_6.$$

Remarque. — Soit OMN le triangle formé par les trois droites de l'un des quatre systèmes dont on vient de prouver l'existence. Supposons, par exemple, que les côtés MN, NO et OM contiennent respectivement les points A_1, A_2, A_3; A_4, A_5, A_6 et A_7, A_8, A_9. En considérant successivement les neuf droites qui forment les trois derniers systèmes et appliquant à chacune de ces droites le théorème connu *des transversales*, on obtient neuf équations, d'où l'on déduit en particulier,

$$\left(\frac{MA_1}{NA_1}\right)^3 = \left(\frac{MA_2}{NA_2}\right)^3 = \left(\frac{MA_3}{NA_3}\right)^3.$$

On conclut de là immédiatement que les neuf points d'inflexion d'une courbe du troisième degré réelle ne peuvent être tous réels; mais il est aisé de voir, en outre, que parmi ces neuf points, six au moins sont imaginaires. En effet, considérons un point d'inflexion imaginaire; par ce point passent quatre droites contenant chacune deux autres points d'inflexion : or, s'il y avait au plus quatre points d'inflexion imaginaires, l'une des quatre droites dont il s'agit contiendrait nécessairement deux points d'inflexion réels, ce qui est impossible; car la droite qui passe par deux points réels d'une courbe du troisième degré rencontre de nouveau la courbe en un troisième point réel.

On voit donc qu'une courbe réelle du troisième degré ne peut avoir plus de trois points d'inflexion réels, lesquels sont toujours en ligne droite, d'après le théorème I. Je dis, en outre, qu'il y a effectivement des courbes du troisième degré qui ont trois points d'inflexinn réels. Par exemple, la courbe dont $\left(\frac{x}{z}, \frac{y}{z}\right)$ désignent les conrdonnées rectilignes et qui a pour équation

$$y = \frac{x^3 - xz^2}{3x^2 + z^2},$$

est rencontrée par l'axe des abscisses en trois points d'inflexion réels.

Théorème III. — *Les coordonnées rectilignes de chacun des neuf points d'inflexion d'une courbe du troisième degré, sont toujours exprimables par des fonctions algébriques explicites des coefficients de l'équation de la conrbe.*

Soit

$$(1) \qquad u = 0$$

l'équation d'une courbe du troisième degré. Les neuf points d'inflexion de cette courbe sont, comme on l'a vu, sur une seconde courbe du troisième degré

$$v = 0,$$

en sorte que si k désigne une constante indéterminée (lemme IV), l'équation

$$(2) \qquad ku + v = 0$$

représentera généralement toutes les courbes du troisième degré qui passent par les neuf points d'inflexion de la proposée. Or nous avons vu qu'on peut faire passer par ces neuf points quatre lignes du troisième degré formées chacune de trois droites; donc il y a quatre valeurs de k pour lesquelles l'équation (2) se décompose en facteurs linéaires. Si l'on cherche à exprimer que la fonction $ku + v$ est le produit de trois facteurs linéaires, on obtiendra trois équations de condition qui devront se réduire à

une seule, et celle-ci sera du quatrième degré par rapport à k (*). Si l'on résout cette équation du quatrième degré, que l'on prenne pour k l'une quelconque de ses racines et qu'ensuite on résolve l'équation (2) par rapport à l'une des coordonnées, on trouvera nécessairement que les trois valeurs de cette coordonnée sont des fonctions linéaires de la deuxième coordonnée. La décomposition de l'équation (2) en facteurs linéaires étant ainsi effectuée, on aura les équations de trois droites contenant chacune trois des neuf points d'inflexion de la proposée, et, pour avoir les coordonnées de ces neuf points, il suffira de chercher successivement les solutions communes à l'équation (1) et à l'équation de chacune des trois droites, ce qui exigera seulement la résolution de trois équations du troisième degré à une inconnue.

Il s'ensuit que les coordonnées des neuf points d'inflexion sont exprimables par des fonctions algébriques explicites des coefficients de l'équation proposée.

Corollaire. — *L'équation du neuvième degré qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré, est toujours résoluble algébriquement.*

Propriété de l'équation du neuvième degré qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré.

Soit

$$(1) \qquad u = 0$$

l'équation d'une courbe du troisième degré entre les coordonnées rectilignes $\frac{x}{z}$ et $\frac{y}{z}$; nous avons vu que les points d'inflexion de cette courbe sont sur une seconde courbe du troisième degré,

$$(2) \qquad v = 0$$

(*) Dans un beau Mémoire publié au tome XXXIX du Journal de M. Crelle, M. Aronhold a obtenu effectivement cette équation du quatrième degré en k, sous une forme bien remarquable. Car les coefficients s'expriment par deux fonctions seulement des coefficients de l'équation de la courbe proposée.



Si l'on élimine y entre les équations (1) et (2), on obtient une équation

$$(3) \qquad \varpi = 0,$$

homogène par rapport à x et z et du neuvième degré. Cette équation, dont les racines $\frac{x}{z}$ représentent les abscisses des points d'inflexion, est toujours résoluble algébriquement, comme nous l'avons vu plus haut. Mais il existe, entre les racines de l'équation (3), des relations remarquables que nous allons faire connaître, d'après M. Hesse, et desquelles ce géomètre a déduit la résolubilité par radicaux de l'équation (3).

Remarquons d'abord que la valeur de $\frac{y}{z}$ correspondante à chaque racine $\frac{x}{z}$ de l'équation (3) peut s'exprimer en fonction rationnelle de $\frac{x}{z}$ et des quantités connues de l'équation (1). Cela résulte immédiatement de la méthode que nous avons exposée dans la quatrième leçon pour la résolution de deux équations simultanées à deux inconnues. D'après cela, les coordonnées de chaque point d'inflexion de la courbe proposée doivent satisfaire à une même équation de la forme

$$(4) \qquad \frac{y}{z} = F\left(\frac{x}{z}\right),$$

où F désigne une fonction rationnelle.

Cela posé, désignons par $\frac{x_1}{z_1}$, $\frac{y_1}{z_1}$ et $\frac{x_2}{z_2}$, $\frac{y_2}{z_2}$ les coordonnées de deux points d'inflexion de la courbe (1); la droite qui passe par ces deux points aura pour équation

$$\frac{\frac{x}{z} - \frac{x_1}{z_1}}{\frac{x}{z} - \frac{x_2}{z_2}} = \frac{\frac{y}{z} - \frac{y_1}{z_1}}{\frac{y}{z} - \frac{y_2}{z^2}}.$$

En désignant par $-\lambda\frac{z_2}{z_1}$ la valeur de chacun des membres, il

vient

$$\frac{x}{z}(z_1 + \lambda z_2) = x_1 + \lambda x_2,$$

$$\frac{y}{z}(z_1 + \lambda z_2) = y_1 + \lambda y_2;$$

on peut disposer de z de manière que l'on ait $z = z_1 + \lambda z_2$, et l'on voit alors que notre droite pourra être représentée par les trois équations suivantes :

$$(5) \qquad x = x_1 + \lambda x_2, \quad y = y_1 + \lambda y_2, \quad z = z_1 + \lambda z_2.$$

Au moyen de ces équations, on obtiendra tous les points de la droite, en donnant à λ toutes les valeurs possibles. Or, d'après le théorème de Maclaurin démontré plus haut, cette droite coupe la courbe (1) en un troisième point d'inflexion; pour avoir la valeur de λ qui convient à ce troisième point, il suffit de porter dans l'équation (1) les valeurs de x, y, z tirées des équations (5), et de résoudre ensuite par rapport à λ. Par cette substitution il vient

$$(6) \left\{ \begin{aligned} &(u)_1 + \lambda\left[x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1\right] \\ &\quad + \lambda^2\left[x_1\left(\frac{du}{dx}\right)_2 + y_1\left(\frac{du}{dy}\right)_2 + z_1\left(\frac{du}{dz}\right)_2\right] + \lambda^3(u)_2 = 0, \end{aligned} \right.$$

les indices 1 et 2 indiquant que, dans les expressions qui en sont affectées, on doit mettre x_1, y_1, z_1 ou x_2, y_2, z_2 à la place de x, y, z. En effet, il résulte immédiatement de la formule de Taylor, qu'après la substitution, les deux premiers termes de u sont

$$(u)_1 + \lambda\left[x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1\right],$$

et il est évident que les deux derniers termes doivent se déduire de ces deux-ci, en changeant $x_1, y_1, z_1, x_2, y_2, z_2$, en λx_2, λy_2, λz_2, $\frac{1}{\lambda}x_1$, $\frac{1}{\lambda}y_1$, $\frac{1}{\lambda}z_1$.

Si l'on supprime les termes $(u)_1$ et $(u)_2$ qui sont nuls, l'équa-

tion (6), divisée par λ, donne la valeur suivante de λ :

$$(7) \qquad \lambda = -\frac{x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1}{x_1\left(\frac{du}{dx}\right)_2 + y_1\left(\frac{du}{dy}\right)_2 + z_1\left(\frac{du}{dz}\right)_2},$$

qui convient au troisième point d'inflexion. Si l'on désigne par $\frac{x_3}{z_3}$, $\frac{y_3}{z_3}$ les coordonnées de ce point, et qu'on porte la valeur de λ, que nous venons de trouver, dans les équations (5), on aura

$$\frac{x_3}{z_3} = \frac{x_1\left[x_1\left(\frac{du}{dx}\right)_2 + y_1\left(\frac{du}{dy}\right)_2 + z_1\left(\frac{du}{dz}\right)_2\right] - x_2\left[x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1\right]}{z_1\left[x_1\left(\frac{du}{dx}\right)_2 + y_1\left(\frac{du}{dy}\right)_2 + z_1\left(\frac{du}{dz}\right)_2\right] - z_2\left[x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1\right]},$$

$$\frac{y_3}{z_3} = \frac{y_1\left[x_1\left(\frac{du}{dx}\right)_2 + y_1\left(\frac{du}{dy}\right)_2 + z_1\left(\frac{du}{dz}\right)_2\right] - y_2\left[x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1\right]}{z_1\left[x_1\left(\frac{du}{dx}\right)_2 + y_1\left(\frac{du}{dy}\right)_2 + z_1\left(\frac{du}{dz}\right)_2\right] - z_2\left[x_2\left(\frac{du}{dx}\right)_1 + y_2\left(\frac{du}{dy}\right)_1 + z_2\left(\frac{du}{dz}\right)_1\right]}.$$

Considérons, en particulier, la première de ces équations : le second membre ne change pas quand on change x_1, y_1, z_1 en x_2, y_2, z_2, et réciproquement; en divisant le numérateur et le dénominateur de ce second membre par $z_1^2 z_2^2$, il prend la forme

$$f\left(\frac{x_1}{z_1}, \frac{y_1}{z_1}, \frac{x_2}{z_2}, \frac{y_2}{z_2}\right),$$

f désignant une fonction rationnelle qui ne change pas quand on transpose les indices 1 et 2. Or, d'après l'équation (4), on a

$$\frac{y_1}{z_1} = F\left(\frac{x_1}{z_1}\right), \quad \frac{y_2}{z_2} = F\left(\frac{x_2}{z_2}\right),$$

F désignant une fonction rationnelle. Donc la valeur de $\frac{x_3}{z_3}$ peut se réduire à la forme suivante,

$$\frac{x_3}{z_3} = \theta\left(\frac{x_1}{z_1}, \frac{x_2}{z_2}\right),$$

θ désignant une fonction rationnelle et symétrique des deux quantités qu'elle renferme. Il est évident que l'équation précédente ne cessera pas d'être exacte si l'on permute les indices 1, 2, 3; car on serait arrivé directement aux équations qu'on obtient par ces permutations, en partant du premier point d'inflexion et du troisième, ou du deuxième et du troisième, au lieu de partir du premier et du deuxième. Donc les abscisses $\frac{x_1}{z_1}$, $\frac{x_2}{z_2}$, $\frac{x_3}{z_3}$ de trois points d'inflexion en ligne droite, satisfont aux trois relations

$$\frac{x_1}{z_1}=\theta\left(\frac{x_2}{z_2},\frac{x_3}{z_3}\right),\quad \frac{x_2}{z_2}=\theta\left(\frac{x_3}{z_3},\frac{x_1}{z_1}\right),\quad \frac{x_3}{z_3}=\theta\left(\frac{x_1}{z_1},\frac{x_2}{z_2}\right),$$

où θ, nous le répétons, désigne une fonction rationnelle et symétrique. De cette propriété résulte, comme on va voir, la solubilité de l'équation (3).

Sur la résolution algébrique d'une classe d'équations du neuvième degré.

Soient

(1) $$\chi(x)=0$$

une équation du neuvième degré et θ une fonction rationnelle et symétrique donnée de deux variables. Si l'équation proposée a cette propriété, que deux racines quelconques x_λ et x_μ fournissent une troisième racine $x_\varkappa$, de telle sorte qu'on ait en même temps

(2) $$x_\varkappa=\theta(x_\lambda, x_\mu),\ x_\lambda=\theta(x_\mu, x_\varkappa),\ x_\mu=\theta(x_\varkappa, x_\lambda),$$

cette équation sera résoluble algébriquement. On voit que l'équation qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré a la propriété dont il s'agit ici.

Soient

$$x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_6,\ x_7,\ x_8,\ x_9$$

les neuf racines de l'équation (1). M. Hesse nomme *racines*

conjuguées trois racines de l'équation (1) qui satisfont aux relations (2). Il est évident que chaque racine fait partie de quatre combinaisons de trois racines conjuguées; par suite, en comptant quatre combinaisons pour chaque racine, on aurait 4×9 ou trente-six combinaisons; mais chacune de ces combinaisons se trouvant répétée trois fois, on voit qu'il n'y a que douze combinaisons distinctes de racines conjuguées. En raisonnant comme nous l'avons fait au sujet de la détermination des douze droits qui passent chacune par trois points d'inflexion d'une courbe du troisième degré, on vera qu'on peut former les quatre groupes suivants, composés de trois combinaisons de racines conjuguées et contenant chacune les neuf racines :

$$(3) \quad \left\{ \begin{array}{lll} x_1 x_2 x_3, & x_4 x_5 x_6, & x_7 x_8 x_9; \\ x_2 x_4 x_7, & x_3 x_5 x_8, & x_1 x_6 x_9; \\ x_5 x_7 x_1, & x_6 x_8 x_2, & x_4 x_9 x_3; \\ x_8 x_1 x_4, & x_9 x_2 x_5, & x_7 x_3 x_6. \end{array} \right.$$

Le nombre total des combinaisons de trois racines est 84; il y a donc soixante-douze combinaisons de trois racines non conjuguées.

Considérons l'un quelconque des quatre groupes (3), et désignons-le par

$$x_\kappa x_\lambda x_\mu, \quad x_{\kappa'} x_{\lambda'} x_{\mu'}, \quad x_{\kappa''} x_{\lambda''} x_{\mu''}.$$

On peut supposer que x_κ, $x_{\kappa'}$, $x_{\kappa''}$ ne soient point conjuguées, et, par suite, on pourra les considérer comme trois racines *quelconques* non conjuguées. Alors, comme rien ne distingue entre eux les indices λ et μ, λ' et μ', λ'' et μ'', on aura ces trois combinaisons de racines conjuguées,

$$x_{\kappa'} x_{\kappa''} x_\lambda, \quad x_{\kappa''} x_\kappa x_{\lambda'}, \quad x_\kappa x_{\kappa'} x_{\lambda''};$$

les six autres combinaisons de racines conjuguées sont alors nécessairement

$$\begin{array}{lll} x_\kappa x_{\mu'} x_{\mu''}, & x_{\kappa'} x_{\mu''} x_\mu, & x_{\kappa''} x_\mu x_{\mu'}; \\ x_{\lambda'} x_{\lambda''} x_\mu, & x_{\lambda''} x_\lambda x_{\mu'}, & x_\lambda x_{\lambda'} x_{\mu''}. \end{array}$$

On voit que les neuf racines sont exprimables en fonction ra-

tionnelle de trois racines non conjuguées quelconques $x_{\varkappa}$, $x_{\nu'}$, $x_{\varkappa''}$; on a effectivement

$$(4)\begin{cases} x_{\varkappa} = x_{\varkappa}, & x_{\lambda} = \theta(x_{\varkappa'}, x_{\varkappa''}), \quad x_{\mu} = \theta[\theta(x_{\varkappa''}, x_{\varkappa}), \theta(x_{\varkappa}, x_{\varkappa'})]; \\ x_{\varkappa'} = x_{\varkappa'}, & x_{\lambda'} = \theta(x_{\varkappa''}, x_{\varkappa}), \quad x_{\mu'} = \theta[\theta(x_{\varkappa}, x_{\varkappa'}), \theta(x_{\varkappa'}, x_{\varkappa''})]; \\ x_{\varkappa''} = x_{\varkappa''}, & x_{\lambda''} = \theta(x_{\varkappa}, x_{\varkappa'}), \quad x_{\mu''} = \theta[\theta(x_{\varkappa'}, x_{\varkappa''}), \theta(x_{\varkappa''}, x_{\varkappa})]. \end{cases}$$

Cela posé, désignons par α une constante indéterminée, et formons la fonction symétrique suivante de trois racines conjuguées quelconques $x_{\varkappa}$, x_{λ}, x_{μ} du troisième degré par rapport à α, savoir:

$$(5) \qquad y_{\varkappa,\lambda,\mu} = (\alpha - x_{\varkappa})(\alpha - x_{\lambda})(\alpha - x_{\mu});$$

quand on remplace $x_{\varkappa}$, x_{λ}, x_{μ} par chacune des douze combinaisons (3), la fonction $y_{\nu,\lambda,\mu}$ prend ces douze valeurs :

$$(6)\begin{cases} y_{1,2,3}, & y_{4,5,6}, & y_{7,8,9}; \\ y_{2,4,7}, & y_{3,5,8}, & y_{1,6,9}; \\ y_{5,7,1}, & y_{6,8,2}, & y_{4,9,3}; \\ y_{8,1,4}, & y_{9,2,5}, & y_{7,3,6}. \end{cases}$$

Formons ensuite la fonction symétrique suivante,

$$(7) \quad z = (\beta - y_{\varkappa,\lambda,\mu})(\beta - y_{\varkappa',\lambda',\mu'})(\beta - y_{\varkappa'',\lambda'',\mu''}),$$

qui est du troisième degré par rapport à l'indéterminée β. Soient z_1, z_2, z_3, z_4 les quatre valeurs que prend z quand on y met successivement pour $y_{\varkappa\,\lambda\,\mu}$, $y_{\varkappa'\,\lambda'\,\mu'}$, $y_{\varkappa''\,\lambda''\,\mu''}$ les quatre groupes de valeurs (6). Formons enfin l'équation du quatrième degré

$$(8) \qquad z^4 + A_1 z^3 + A_2 z^2 + A_3 z + A_4 = 0,$$

qui a pour racines z_1, z_2, z_3, z_4.

Je dis que les coefficients de l'équation (8) sont exprimables rationnellement en fonction des quantités connues de l'équa-

tion (1) et de la fonction θ. En effet, on a

$$(9)\qquad \begin{cases} y_{\kappa\ \lambda\ \mu} = (\alpha - x_\nu)(\alpha - x_\lambda)(\alpha - x_\mu), \\ y_{\kappa'\ \lambda'\ \mu'} = (\alpha - x_{\kappa'})(\alpha - x_{\lambda'})(\alpha - x_{\mu'}), \\ y_{\kappa''\ \lambda''\ \mu''} = (\alpha - x_{\kappa''})(\alpha - x_{\lambda''})(\alpha - x_{\mu''}); \end{cases}$$

en portant ces valeurs dans l'équation (7) et se servant des équations (4), on aura la valeur de z exprimée en fonction rationnelle de trois racines non conjuguées x_κ, $x_{\kappa'}$, $x_{\nu''}$, savoir :

$$(10)\qquad z = \psi(x_\kappa, x_{\kappa'}, x_{\kappa''}),$$

et cette fonction ψ sera symétrique par rapport à x_κ, $x_{\kappa'}$, $x_{\kappa''}$; car il est aisé de voir, d'après les équations (4), qu'en permutant ces trois racines, les quantités $y_{\kappa,\lambda,\mu}$, $y_{\nu'\ \lambda'\ \mu'}$, $y_{\kappa''\ \lambda''\ \mu''}$ ne font que se changer les unes dans les autres, ce qui ne change pas la valeur de z.

Élevons le second membre de l'équation (10) à une puissance entière quelconque de degré m ; désignons par

$$\sum\nolimits'' \psi(x_\kappa, x_{\nu'}, x_{\kappa'})^m$$

la somme des termes qu'on deduit de $\psi(x_\kappa\ x_{\kappa'}\ x_{\kappa''})^m$ en prenant successivement pour $x_\kappa\ x_{\kappa'}\ x_{\kappa''}$ les soixante-douze combinaisons de trois racines non conjuguées; par $\sum' \psi(x_\kappa\ x_{\kappa'}\ x_{\kappa''})^m$ la somme des termes qu'on déduit de $\psi(x_\kappa\ x_{\kappa'}\ x_{\kappa''})^m$ en prenant successivement pour $x_\kappa\ x_{\kappa'}\ x_{\kappa''}$ les douze combinaisons de racines conjuguées; enfin par $\sum \psi(x_\kappa\ x_{\kappa'}\ x_{\kappa''})^m$ la somme de tous les termes qu'on déduit de $\psi(x_\kappa\ x_{\kappa'}\ x_{\kappa''})^m$ en prenant pour $x_\kappa\ x_{\kappa'}\ x_{\kappa''}$ toutes les quatre-vingt-quatre combinaisons de trois racines.

On aura

$$(11)\quad \left\{\begin{array}{l} \sum'' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m + \sum' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m \\ = \sum \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m. \end{array}\right.$$

Le second membre de cette équation (10) est une fonction rationnelle et symétrique de toutes les racines, et l'on peut, par conséquent, l'exprimer en fonction rationnelle des quantités connues. Il en est de même de $\sum' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m$; en effet, $x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''}$ étant ici des racines conjuguées, on a

$$\begin{array}{l} \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m = \psi[x_\varkappa\, x_{\varkappa'}\, \theta(x_\varkappa\, x_{\varkappa'})]^m \\ = \psi[x_{\varkappa'}\, x_{\varkappa''}\, \theta(x_{\varkappa'}\, x_{\varkappa''})]^m = \psi[x_{\varkappa''}\, x_{\varkappa'}\, \theta(x_{\varkappa''}\, x_{\varkappa'})]^m; \end{array}$$

d'où il suit que $\sum' \psi(x_\varkappa\, x_\varkappa\, x_{\varkappa''})^m$ est égale au tiers de la somme des trente-six valeurs que prend $\psi[x_\varkappa\, x_{\varkappa'}\, \theta(x_\varkappa\, x_{\varkappa'})]^m$ quand on prend pour $x_\varkappa$, $x_{\varkappa'}$ les trente-six combinaisons de deux racines. En désignant cette somme par le signe $\sum$, on a

$$(12)\quad \sum' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m = \frac{1}{3}\sum \psi[x_\varkappa\, x_{\varkappa'}\, \theta(x_\varkappa\, x_{\varkappa'})]^m,$$

et, par suite,

$$(13)\quad \left\{\begin{array}{l} \sum'' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m = \sum \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m \\ -\frac{1}{3}\sum \psi[x_\varkappa\, x_{\varkappa'}\, \theta(x_\varkappa\, x_{\varkappa'})]^m, \end{array}\right.$$

ce qui montre que $\sum'' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})$ est une fonction rationnelle et symétrique de toutes les racines; on peut donc l'exprimer en fonction rationnelle des quantités connues. Si maintenant on remarque qu'aux soixante-douze combinaisons de racines non conjuguées, répondent seulement quatre

valeurs de la fonction z^m, savoir, z_1^m, z_2^m, z_3^m, z_4^m et que chacune de ces valeurs revient dix-huit fois, on verra que l'on a

$$(14) \qquad z_1^m + z_2^m + z_3^m + z_4^m = \frac{1}{18} \sum\nolimits'' \psi(x_\varkappa\, x_{\varkappa'}\, x_{\varkappa''})^m.$$

En donnant au nombre m les valeurs 1, 2, 3, 4, on obtiendra, par l'équation (14), les sommes de puissances semblables des racines de l'équation (8) qui sont nécessaires pour calculer les coefficients A_1, A_2, A_3, A_4 ; on voit que ces coefficients se trouvent ainsi exprimés en fonction rationnelle des quantités connues.

Voici maintenant comment on obtiendra les racines de l'équation (1). On cherchera une racine quelconque de l'équation (8). Cette racine sera, d'après ce qui précède, une fonction entière et du troisième degré de l'indéterminée θ ; en égalant à zéro cette racine, on aura une équation du troisième degré en θ dont les racines seront les trois quantités qui forment l'un des quatre groupes (6). En égalant à zéro une de ces nouvelles racines, on aura une équation du troisième degré par rapport à l'indéterminée α ; les trois valeurs de α racines de cette équation seront trois racines conjuguées de l'équation (1). Pour avoir toutes les racines de l'équation (1), il suffit de traiter de la même manière toutes les racines de l'équation (8).

NOTE XIII.

SUR LES ÉQUATIONS RÉSOLUBLES ALGÉBRIQUEMENT.

La Note qu'on va lire renferme la traduction textuelle d'un Mémoire que M. Léopold Kronecker vient de publier, et qui a été communiqué par M. Lejeune-Dirichlet à la classe des Sciences mathématiques et physiques de l'Académie de Berlin, le 20 juin 1853.

« Les recherches entreprises jusqu'à présent sur la possibilité de résoudre les équations de degré premier, et particulièrement celles d'Abel et de Galois qui ont servi de point de départ à tous les travaux ultérieurs sur le même objet, ont eu pour principal résultat de conduire à deux critérium à l'aide desquels on pût juger si une équation donnée est résoluble ou non. Mais, à vrai dire, ces critérium ne fournissaient pas la moindre lumière sur la nature même des équations résolubles. On ne savait même pas si, en outre des équations traitées par Abel dans le tome IV du Journal de Crelle (*), et de celles qui se ramènent immédiatement aux équations binômes, on ne savait pas, dis-je, s'il existait d'autres équations satisfaisant aux conditions données de résolubilité. Encore moins savait-on former de pareilles équations, et dans aucune recherche mathématique on n'en avait rencontré. Ajoutons que ces deux théorèmes bien connus d'Abel et de Galois sur les équations résolubles étaient plus propres à en cacher la vraie nature qu'à nous la découvrir, ainsi que je le montrerai plus particulièrement à l'égard de l'un de ces critérium. Le caractère propre des équations résolubles restait donc dans une sorte d'obscurité, et le seul travail qui jette quelque lumière sur ce point, savoir, une Notice d'Abel sur les racines des équations du cinquième

(*) *Voir* la vingt-septième leçon.

degré à coefficients entiers, semble avoir été peu remarqué, sans doute à cause de son objet tout spécial. Mais la question ne pouvait être complétement éclaircie que par la solution du problème suivant : *Trouver toutes les équations résolubles*. Car, une fois cette solution obtenue, non-seulement on peut trouver une infinité de nouvelles équations résolubles, mais on a en quelque sorte devant les yeux toutes celles qui le sont, et à l'aide de la forme explicite de leurs racines on peut trouver et démontrer toutes leurs propriétés.

» A ces remarques sur le but et sur le résultat de mes recherches, je dois ajouter que pour rendre la solution possible il fallait encore transformer complétement le problème qui vient d'être posé. La manière de formuler la question est, en effet, de la plus grande importance, et de peur que la brièveté ne nuise à la clarté, je m'étendrai un peu sur ce point.

» Abel, dans un Mémoire dont nous ne possédons que des fragments (tome II, *OEuvres complètes*, n° XV), s'est proposé, entre autres problèmes, celui-ci : *Trouver l'expression algébrique la plus générale qui puisse satisfaire à une équation algébrique d'un degré donné*. Si l'on ajoute à cet énoncé ce qui est nécessaire pour rendre la question déterminée, il comprend tous les problèmes qu'on peut se proposer sur la résolution des équations, et il est le plus général qu'on doive substituer à ce problème impossible : *Exprimer en fonction algébrique des coefficients la racine d'une équation de degré quelconque*. Mais, ainsi qu'on vient de le dire, il fallait rendre la question déterminée en précisant la manière dont l'expression cherchée doit dépendre des coefficients de l'équation : il convient donc de la poser comme il suit :

» *Trouver la fonction la plus générale de quantités données quelconques* A, B, C, *etc., qui satisfasse à une équation d'un degré donné dont les coefficients sont des fonctions rationnelles de ces quantités.*

» Observons qu'on doit supposer ici l'équation irréductible relativement à A, B, C, etc., c'est-à-dire que A, B, C, etc., restant quelconques, l'équation ne doit pas pouvoir se dé-

composer en facteurs d'un degré moindre dont les coefficients soient des fonctions rationnelles de A, B, C, etc. Cela posé, le problème précédent peut s'énoncer de cette manière :

« *Étant donné un nombre entier n, trouver la fonction algébrique la plus générale de* A, B, C, *etc., telle que, parmi les expressions qu'on en déduit en attribuant aux radicaux leurs diverses valeurs, il y en ait n dont les fonctions symétriques soient rationnelles en* A, B, C, *etc.*

» Ce nombre n est aussi le degré de l'équation qui a pour racines les n expressions dont on vient de parler : dans le cas où il est premier, Abel, dans le Mémoire cité, est parvenu à donner les deux formes suivantes aux expressions algébriques cherchées. La première est

$$(1) \qquad p_0 + s^{\frac{1}{\mu}} + f_2(s).\, s^{\frac{2}{\mu}} + \ldots + f_{\mu-1}(s)\, s^{\frac{\mu-1}{\mu}}$$

(tome II des *Œuvres complètes*, page 204), où μ désigne le degré supposé premier de l'équation, p_0 une fonction rationnelle de A, B, C, etc., s une fonction algébrique des mêmes quantités, et $f_i(s)$ une fonction rationnelle de s et de A, B, C, etc. La seconde forme, qu'on trouve à la page 190 du même volume, est

$$(2) \qquad p_0 + R_1^{\frac{1}{\mu}} + R_2^{\frac{1}{\mu}} + \ldots R_{\mu-1}^{\frac{1}{\mu}},$$

où p_0 est une fonction rationnelle de A, B, C, etc., et où R_1, R_2, etc., sont les racines d'une équation du degré $\mu - 1$ dont les coefficients sont des fonctions rationnelles de A, B, C, etc. M. Malmsten a donné de ces deux formes une démonstration étendue (tome XXXIV du Journal de Crelle), mais qui aurait besoin, si je ne me trompe, d'être complétée dans quelques-unes de ses parties.

» Il est bien vrai que toute fonction algébrique, satisfaisant au problème proposé, doit pouvoir se mettre sous ces deux formes; mais ces formes sont encore trop générales, c'est-à-dire qu'elles renferment des fonctions algébriques qui ne répondent pas à la

question. Je les ai donc étudiées de plus près, et j'ai trouvé d'abord que parmi les fonctions renfermées dans la forme (2), celles qui satisfont au problème proposé doivent avoir la propriété non-seulement que les fonctions symétriques de R_1, R_2, etc., soient rationnelles en A, B, C, etc. (ce qu'Abel a remarqué), mais aussi que les fonctions cycliques des quantités R_1, R_2, etc., prises dans un certain ordre, soient également rationnelles en A, B, C, etc. : en d'autres termes, *l'équation de degré* $\mu - 1$, *dont* R_1, R_2, *etc., sont les racines, doit être une équation abélienne.* J'entendrai toujours ici par équations abéliennes cette classe particulière d'équations résolubles qu'Abel a considérées dans le Mémoire XI du premier volume des *Œuvres complètes*, et dont je supposerai les coefficients fonctions rationnelles de A, B, C, etc. En désignant par $x_1, x_2, \ldots, x_n$ des racines prises dans un ordre déterminé, ces équations peuvent être définies soit en disant que les fonctions cycliques des racines sont rationnelles en A, B, C, etc. (*), soit en disant qu'on a les relations

$$x_2 = \theta(x_1), \quad x_3 = \theta(x_2), \ldots, \quad x_n = \theta(x_{n-1}), \quad x_1 = \theta(x_n),$$

où $\theta(x)$ est une fonction entière de x dont les coefficients sont rationnels en A, B, C, etc. Nous reviendrons tout à l'heure sur ces équations dont la considération est du plus haut intérêt au point de vue de l'analyse et de la théorie des nombres, et aussi, comme on le voit, au point de vue de l'algèbre proprement dite.

Un nouvel examen des formes (1) et (2) fournit encore une détermination plus précise des quantités R qui figurent dans la seconde. On doit avoir, en effet,

$$(3) \qquad R_\varkappa = F(r_\varkappa)^\mu . r_\varkappa^{\gamma-1} . r_{\varkappa+1}^{\gamma-2} . r_{\varkappa+2}^{\gamma-3} \ldots r_{\varkappa+\mu-2},$$

(*) On nomme fonction *cyclique* de n quantités $r_1, r_2, \ldots, r_n$, l'expression

$$(x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{n-1} x_n)^n,$$

où α est racine de $\alpha^n = 1$.

où r_x, r_{x+1}, etc., sont les $\mu-1$ racines d'une équation abélienne quelconque du degré $\mu-1$, c'est-à-dire où les fonctions symétriques et les fonctions cycliques des quantités r (prises dans l'ordre des indices) sont rationnelles en A, B, C, etc., où, de plus, $F(r)$ est une fonction rationnelle de r et de A, B, C, etc., et où enfin γ_m désigne le plus petit reste positif de g^m suivant le module μ, g étant une racine primitive de μ. Si l'on substitue cette valeur de R_x dans l'expression (2), on obtient une forme qui non-seulement renferme toutes les expressions satisfaisant au problème, mais (ce qui est ici le plus essentiel) n'en renferme pas d'autres. En d'autres termes, la forme ainsi obtenue vérifie identiquement une équation du degré μ dont les coefficients sont des fonctions rationnelles de A, B, C, etc. Les autres racines s'obtiennent par la combinaison des diverses valeurs des radicaux $\mu^{\text{ièmes}}$ dans la forme (2), de façon que la $m^{\text{ième}}$ racine z_m est donnée par la formule

$$(4)\quad z_m = p_0 + \omega^m R_1^{\frac{1}{\mu}} + \omega^{gm} R_2^{\frac{1}{\mu}} + \omega^{g^2 \cdot m} R_3^{\frac{1}{\mu}} + \ldots + \omega^{g^{\mu-2} \cdot m} R_{\mu-1}^{\frac{1}{\mu}},$$

ω désignant une racine $\mu^{\text{ième}}$ imaginaire de l'unité, et les quantités R étant déterminées par la formule (3).

» De là, il suit d'abord que, tandis que les fonctions symétriques des quantités z sont rationnelles en A, B, C, etc., les fonctions cycliques des mêmes quantités prises dans l'ordre des indices sont des fonctions rationnelles de A, B, C, etc., de r_1, r_2, etc., et de ω. On voit par là que : *toute équation résoluble algébriquement d'un degré premier μ est une équation abélienne, quand on regarde comme connue une quantité ρ_1 qui elle-même est racine d'une équation abélienne du degré $\mu-1$*, ou bien encore que *les μ racines d'une équation résoluble sont toujours liées entre elles de façon que l'on ait*

$$z_2 = f(z_1, \rho_1), \quad z_3 = f(z_2, \rho_1), \ldots, \quad z_1 = f(z_\mu, \rho_1),$$

où $f(z, \rho_1)$ désigne une fonction rationnelle de z, de ρ_1 et de

A, B, C, *etc.* (*), *et où* ρ_1 *est la racine d'une équation abélienne dont les coefficients sont des fonctions rationnelles de* A, B, C, *etc.* Cette relation entre les racines de toute équation résoluble est d'ailleurs la vraie source de la propriété assignée par Abel et Galois comme le caractère spécial des équations résolubles d'un degré premier, savoir : *que chaque racine doit être une fonction rationnelle de deux autres.* Parmi les conséquences intéressantes qui découlent des résultats précédents, je me bornerai à une seule : c'est que la quantité r_1, en tant que racine d'une équation abélienne du degré $\mu - 1$, ne contenant que des radicaux dont les indices sont diviseurs de $\mu - 1$, ou pouvant être ramenée à n'en contenir que de tels, la racine elle-même de toute équation résoluble pourra s'exprimer par les radicaux dont on vient de parler et par des radicaux d'indice μ. Abel (autant que je le sache) n'a fait cette importante remarque que pour $\mu = 5$ et, pour ce cas, il a donné la forme la plus générale de la racine d'une équation résoluble (tome II des *Œuvres complètes*, page 253). Mais il faut observer qu'il s'est borné, dans cette recherche, aux équations dont les coefficients sont des nombres entiers.

» Le problème primitif est maintenant ramené, en vertu de l'équation (3), à trouver la forme la plus générale de la quantité ou, pour mieux dire, de l'expression r_1. D'après ce qu'on a établi ci-dessus au sujet de r_1, r_2, etc., ce second problème peut s'énoncer ainsi :

» *Le nombre n étant donné, trouver la forme la plus générale d'une fonction algébrique de* A, B, C, *etc., telle que, parmi les diverses expressions qui résultent de la combinaison des valeurs des radicaux dans cette fonction, il y en ait n dont les fonctions symétriques et cycliques (celles-ci étant relatives à un ordre déterminé des n expressions) soient rationnelles en* A, B, C, *etc.*

(*) J'ai fait dans ce passage quelques corrections qui m'ont été indiquées par M. Kronecker lui-même. La quantité que nous représentons ici par ρ_1 se trouve désignée, à tort, dans les *Comptes rendus* de l'Académie des Sciences de Berlin, par la lettre r_1. Cette nouvelle racine ρ_1 dépend de la racine r_1 d'une manière très-simple; toutefois ces deux quantités sont différentes entre elles.



» Et l'on voit que ce second problème, énoncé en gros pour ainsi dire, revient *à trouver toutes les équations abéliennes*, comme le problème primitif consistait, en quelque sorte, *à trouver toutes les équations résolubles.*

» En traitant ce second problème, on se trouve ramené à distinguer les cas où n est un nombre premier, ou une puissance de nombre premier, ou un nombre composé quelconque : mais ce dernier cas se ramène aux deux autres; car la solution du problème pour un nombre composé n s'obtient dès qu'on l'a résolu pour les cas où le degré de l'équation abélienne est une des puissances de nombre premier contenues dans n. D'ailleurs, à part quelques complications, le problème n'offre pas plus de difficultés pour une puissance de nombre premier que pour un nombre premier. Seulement, dans le cas le plus simple en apparence, où n est égal au cube ou à une puissance plus élevée de 2, la méthode que j'ai employée avec succès dans tous les autres cas ne suffit plus à la solution complète du problème, et je n'ai pas encore trouvé la modification qu'elle exige alors. Comme la solution du problème primitif pour le nombre premier μ exige la solution du second problème pour $n = \mu - 1$, je ne pourrais donc, jusqu'à présent, donner le résultat complet que pour les nombres premiers μ qui ne sont pas de la forme $8h + 1$. Il suffira, du reste, au but de cette communication préliminaire et pour éclaircir la matière, d'examiner ici le cas du second problème, où n est un nombre premier impair. Je ne donnerai pas seulement le résultat relatif à ce cas, mais j'indiquerai brièvement la méthode qui m'y a conduit, attendu qu'elle est extrêmement simple et qu'elle fournit les principes essentiels pour la solution de ce second problème dans les autres cas, et aussi pour la solution du problème primitif.

» En conservant les notations employées par Abel (dans le Mémoire n° XI déjà cité du tome Ier des *OEuvres complètes*), et en ayant égard à la définition déjà donnée des équations abéliennes, on peut énoncer comme il suit le problème dont il s'agit :

» *Trouver la fonction algébrique la plus générale* z_0 *de* A, B, C, *etc.*, *satisfaisant à une équation du* $n^{ième}$ *degré*, *et telle que*

cette fonction z_0 et les autres racines $z_1, z_2, \ldots, z_{n-1}$ de l'équation vérifient les relations

$$z_1 = \theta(z_0), \quad z_2 = \theta(z_1), \ldots, \quad z_0 = \theta(z_{n-1}),$$

où $\theta(z)$ est une fonction rationnelle de z et de A, B, C, *etc.*

» Admettons que n soit un nombre premier, et adoptant une notation introduite par M. Jacobi, posons

$$z_0 + z_1\alpha + z_2\alpha^2 + \ldots + z_{n-1}\alpha^{n-1} = (\alpha, z),$$

où α désigne une racine $n^{ième}$ de l'unité; nous aurons

$$(5)\quad nz_\varkappa = (1, z) + \alpha^{-\varkappa}(\alpha, z) + \alpha^{-2\varkappa}(\alpha^2, z) + \ldots + \alpha^{-(n-1)\varkappa}(\alpha^{n-1}, z).$$

En suivant la marche tracée par Abel, on montrera ensuite que, pour tout nombre entier $\varkappa$, on a les équations

$$(6)\quad \begin{cases} (\alpha, z)^\varkappa = (\alpha^\varkappa, z)\,\varphi(\alpha), \quad (\alpha^2, z)^\varkappa = (\alpha^{2\varkappa}, z)\,\varphi(\alpha^2), \\ (\alpha^3, z)^\varkappa = (\alpha^{3\varkappa}, z)\,\varphi(\alpha^3), \ldots, \end{cases}$$

où $\varphi(\alpha)$ est une fonction rationnelle de α et de A, B, C, etc.

» Si maintenant on met pour $\varkappa$ une racine primitive g du nombre premier n, tellement choisie que $g^{n-1} - 1$ ne soit divisible par aucune puissance de n plus élevée que la première, on obtiendra des équations de cette forme,

$$(\alpha, z)^g = (\alpha^g, z) f(\alpha), \quad (\alpha^g, z)^g = (\alpha^{g^2}, z) f(\alpha^g), \ldots,$$
$$(\alpha^{g^{n-2}}, z)^g = (\alpha, z) f(\alpha^{g^{n-2}}).$$

Élevons la première de ces équations à la puissance g^{n-2}, la seconde à la puissance g^{n-3}, et ainsi de suite, puis multiplions-les membre à membre; il viendra

$$(7)\qquad (\alpha, z)^{g^{n-1}-1} = f(\alpha)^{g^{n-2}} f(\alpha^g)^{g^{n-3}} \ldots f(\alpha^{g^{n-2}}).$$

Posons à présent

$$g^{n-1} - 1 = m.n,$$

m n'étant pas divisible par n, d'après la supposition précédem-

ment faite; nous aurons, en vertu de l'équation (6),

$$(\alpha, z)^{\varepsilon^{n-1}-1} = (\alpha, z)^{mn} = (\alpha^m, z)^n \varphi(\alpha)^n,$$

et, en substituant dans l'équation (7), nous trouverons

$$(\alpha^m, z)^n \varphi(\alpha)^n = f(\alpha)^{\varepsilon^{n-2}} . f(\alpha\varepsilon)^{\varepsilon^{n-3}} \ldots f(\alpha\varepsilon^{n-2}),$$

résultat qui subsiste pour chacune des valeurs de α, comme on peut le démontrer, et qu'on mettra aisément sous cette forme,

$$(8) \quad (\alpha^m, z) = \mathrm{F}(\alpha^m) \left\{ f(\alpha^m) . f(\alpha^{2m})^{\frac{1}{2}} . f(\alpha^{3m})^{\frac{1}{3}} \ldots f[\alpha^{(n-1)m}]^{\frac{1}{n-1}} \right\}^{\frac{1}{n}}.$$

» Ici il faut entendre par chacun des exposants fractionnaires contenus dans la parenthèse, non pas cet exposant lui-même, mais son plus petit résidu positif relativement au module n; d'ailleurs $\mathrm{F}(\alpha)$ désigne comme $f(\alpha)$ une fonction rationnelle de α et de A, B, C, etc. Cette expression de (α^m, z) étant substituée dans l'équation (5), on obtient une forme que z_x doit nécessairement avoir, et qui satisfait toujours au problème, quelles que soient les fonctions rationnelles de α et de A, B, C, etc., qu'on prenne pour $f(\alpha)$ et $\mathrm{F}(\alpha)$.

» La comparaison de ce résultat avec la forme générale donnée ci-dessus des racines d'une équation résoluble du degré μ, conduit à des propositions intéressantes : mais des conséquences plus intéressantes encore se tirent de la comparaison de l'expression (8), en y supposant que A, B, C, etc., soient des nombres entiers, avec l'expression correspondante que fournissent certaines équations abéliennes qui se présentent dans la théorie de la division du cercle, particulièrement avec la forme très-remarquable donnée pour (α, x), par M. Kummer (Journal de Crelle, tome XXXV, page 363). Cette comparaison fournit en effet le théorème suivant, qui a lieu non-seulement pour un degré premier, mais dans tous les cas, savoir que :

» *Les racines de toute équation abélienne à coefficients entiers peuvent être exprimées rationnellement au moyen des racines de l'unité.*

» Ainsi, ces équations abéliennes générales ne sont rien autre chose en réalité que les équations de la division du cercle.

» Il existe une relation pareille entre les racines des équations abéliennes dont les coefficients sont des nombres complexes de la forme $a + b\sqrt{-1}$ et les racines des équations qui se présentent dans la division de la lemniscate : on peut généraliser ce résultat et l'étendre à toutes les équations abéliennes dont les coefficients contiennent des nombres irrationnels déterminés et racines d'équations algébriques.

» J'ajoute encore une remarque : si l'on applique à la forme (3) le théorème précédent sur les racines des équations abéliennes à coefficients entiers, on trouve que la racine de toute équation résoluble du degré μ à coefficients entiers peut être regardée comme une somme de racines $\mu^{\text{ièmes}}$ de nombres complexes rationnels formés avec les racines de l'unité. Ainsi, la forme nécessaire et suffisante la plus générale de toute racine d'une équation résoluble du degré μ à coefficients entiers s'exprime au moyen de ces nombres complexes : toutefois, la recherche effective de cette forme exige une suite de propositions sur les nombres qui dépasseraient les bornes de cette communication. »

Note relative au précédent Mémoire.

Mon ami, M. Hermite, m'a communiqué une démonstration très-simple de l'un des théorèmes de Galois dont il est parlé dans le Mémoire de M. Kronecker ; je crois faire une chose utile en la reproduisant ici. Le théorème dont il s'agit consiste en ce que :

Étant données deux quelconques des racines d'une équation irréductible de degré premier, soluble par radicaux, les autres s'en déduisent rationnellement.

Lemme I. — *Soient*

$$F(x) = 0$$

une équation irréductible de degré quelconque n, et

$$x_0, x_1, x_2, \ldots, x_{n-1}$$

ses n racines. Si toutes les fonctions des racines invariables par

les substitutions de la forme x_k, x_{k+1} (les indices étant pris, comme fait Galois, suivant le module n) *sont rationnellement connues, on pourra déterminer rationnellement une fonction entière* $\varphi(x)$ *du degré* $n-1$, *telle que l'on ait*

$$x_1 = \varphi(x_0),\ x_2 = \varphi(x_1), \ldots,\ x_{k+1} = \varphi(x_k), \ldots,\ x^{n-1} = \varphi(x_0).$$

On a, en effet,

$$F(x) = (x - x_0)(x - x_1) \ldots (x - x_{n-1}),$$

et, si l'on pose

$$\varphi(x) = \frac{F(x)}{x - x_0} \cdot \frac{x_1}{F'(x_0)} + \frac{F(x)}{x - x_1} \cdot \frac{x_2}{F'(x_1)} + \ldots + \frac{F(x)}{x - x_{n-1}} \cdot \frac{x_0}{F'(x_{n-1})},$$

il est évident que $\varphi(x)$ sera une fonction entière du degré $n-1$ en x et que ses coefficients seront des fonctions des racines invariables par les substitutions de la forme x_k, x_{k+1}; on voit aussi immédiatement que l'on a

$$\varphi(x_0) = x_1,\ \varphi(x_1) = x_2, \ldots,$$

ce qui démontre la proposition énoncée.

Lemme II. — *Si une équation irréductible de degré premier* n *est telle, que toutes les fonctions des racines invariables par les substitutions de la forme* x_k, x_{k+1}, *et de la forme* x_k, $x_{\rho k}$, ρ *désignant une racine primitive de* n, *soient rationnellement connues, on pourra déterminer rationnellement une fonction entière* $\varphi(x)$ *de degré* $n-1$, *telle que l'on ait*

$$\left(x_1 + \lambda x_{\rho} + \lambda^2 x_{\rho^2} + \ldots + \lambda^{n-2} x_{\rho^{n-2}}\right)^{n-1} = \varphi(x_0),$$
$$\left(x_2 + \lambda x_{\rho+1} + \lambda^2 x_{\rho^2+1} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+1}\right)^{n-1} = \varphi(x_1),$$
. . . .
$$\left(x_n + \lambda x_{\rho+n-1} + \lambda^2 x_{\rho^2+n-1} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+n-1}\right)^{n-1} = \varphi(x_{n-1}),$$

les indices étant pris toujours suivant le module n *et* λ *désignant une racine de l'équation binôme* $\lambda^{n-1} = 1$.



Pour démontrer cette proposition, nous ferons voir que le système des équations linéaires ainsi posées entre les coefficients indéterminés de la fonction φ, n'est pas altéré lorsqu'à la place d'une racine quelconque x_k on met x_{k+1} et aussi quand on remplace x_k par $x_{\rho k}$.

Le premier point est évident, puisque chaque équation se déduit de la précédente, en ajoutant une unité aux indices des racines, et qu'en opérant de la sorte sur la dernière on reproduit la première.

Le second point se vérifie aussi immédiatement par rapport à l'équation

$$\left(x_1 + \lambda x_\rho + \lambda^2 x_{\rho^2} + \ldots + \lambda^{n-2} x_{\rho^{n-2}}\right)^{n-1} = \varphi(x_0),$$

car la $(n-1)^{ième}$ puissance de la fonction linéaire

$$x_1 + \lambda x_\rho + \lambda^2 x_{\rho^2} + \ldots + \lambda^{n-2} x_{\rho^{n-2}}$$

ne change pas quand on multiplie cette fonction par λ; or cela revient à multiplier les indices des racines par ρ, ce qui ne change pas non plus le second membre $\varphi(x_0)$ Mais les autres équations du système ne se comportent plus de même. Dans l'une quelconque d'entre elles

$$\left(x_{1+\alpha} + \lambda x_{\rho+\alpha} + \lambda^2 x_{\rho^2+\alpha} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+\alpha}\right)^{n-1} = \varphi\left(x_\alpha\right),$$

faisons $\alpha \equiv \rho^\mu$ (mod. n), ce qui est possible, puisque α ne reçoit plus la valeur zéro ; il viendra

$$(1)\quad \left(\begin{array}{l} x_{1+\rho^\mu} + \lambda x_{\rho+\rho^\mu} + \lambda^2 x_{\rho^2+\rho^\mu} + \ldots \\ \qquad\qquad + \lambda^{n-2} x_{\rho^{n-2}+\rho^\mu} \end{array}\right)^{n-1} = \varphi\left(x_{\rho^\mu}\right),$$

et, en multipliant les indices par ρ,

$$(2)\quad \left(\begin{array}{l} x_{\rho+\rho^{\mu+1}} + \lambda x_{\rho^2+\rho^{\mu+1}} + \lambda^2 x_{\rho^3+\rho^{\mu+1}} + \ldots \\ \qquad\qquad + \lambda^{n-2} x_{\rho^{n-1}+\rho^{\mu+1}} \end{array}\right)^{n-1} = \varphi\left(x_{\rho^{\mu+1}}\right).$$

Or la $(n-1)^{ième}$ puissance de la fonction linéaire

$$x_{\rho+\rho^{\mu+1}} + \lambda x_{\rho^2+\rho^{\mu+1}} + \ldots + \lambda^{n-1} x_{\rho^{n-1}+\rho^{\mu+1}}$$

ne change pas quand on multiplie cette fonction par λ; au lieu de l'équation (2) on peut donc écrire la suivante :

$$\left(\begin{array}{c} x_{\rho^{n-1}+\rho^{\mu+1}} + \lambda x_{\rho+\rho^{\mu+1}} + \lambda^2 x_{\rho^2+\rho^{\mu+1}} + \ldots \\ + \lambda^{n-2} x_{\rho^{n-2}+\rho^{\mu+1}} \end{array}\right)^{n-1} = \varphi\left(x_{\rho^{\mu+1}}\right).$$

Or, en remarquant que $\rho^{n-1} \equiv 1 \pmod{n}$, on reconnaît que celle-ci se déduit de l'équation (1) par le changement de μ en $\mu+1$.

Il suit de là que la substitution $x_k, x_{\rho k}$, ne fait que permuter circulairement nos équations, rangées, à partir de la seconde, suivant l'ordre des valeurs croissantes de μ. En les résolvant par rapport aux coefficients de φ, on sera conduit à des fonctions rationnelles des racines, invariables par les substitutions x_k, x_{k+1} et x_k, $x_{\rho k}$; de sorte que ces coefficients s'exprimeront bien rationnellement, comme nous l'avons annoncé. Notre lemme est donc démontré, et on en déduit le suivant :

Lemme III. — *Si une équation de degré premier est résoluble algébriquement, l'équation de degré moindre d'une unité, qu'on forme en divisant son premier membre par un de ses facteurs linéaires, appartient à la classe des équations nommées abéliennes par M. Kronecker.*

En effet, relativement à l'équation de degré $n-1$, qu'on obtient par la suppression du facteur $x - x_\alpha$, et dont les racines ont été représentées par

$$x_{1+\alpha}, \quad x_{\rho+\alpha}, \quad x_{\rho^2+\alpha}, \ldots, \quad x_{\rho^{n-2}+\alpha},$$

on connaît *rationnellement* la fonction résolvante

$$\left(x_{1+\alpha} + \lambda x_{\rho+\alpha} + \lambda^2 x_{\rho^2+\alpha} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+\alpha}\right)^{n-1}.$$

Les trois lemmes que nous venons de démontrer permettent

maintenant d'établir très-aisément le théorème que nous avons en vue. Faisons, pour un instant,

$$x_{\rho^k + \alpha} = X_k.$$

Puisque nous connaissons (lemme III), en fonction rationnelle de x_α, l'expression

$$(X_0 + \lambda X_1 + \lambda^2 X_2 + \ldots + \lambda^{n-2} X_{n-2})^{n-1},$$

nous devons pareillement regarder comme connue toute fonction rationnelle des racines X_k, invariable par les substitutions de la forme X_k, X_{k+1}. Ceci nous place dans les conditions du lemme I; ainsi nous pouvons former une fonction φ telle, qu'on ait généralement

$$X_{k+1} = \varphi(X_k).$$

D'ailleurs, les coefficients de cette fonction s'exprimeront rationnellement par les quantités connues et la racine x_α; de sorte qu'en mettant cette racine en évidence, nous aurons

$$X_{k+1} = \varphi\left(X_k,\ x_\alpha\right),$$

ou

$$x_{\rho^{k+1} + \alpha} = \varphi\left(x_{\rho^k + \alpha},\ x_\alpha\right).$$

Or on peut prendre $\rho^k = 6$, 6 étant un entier arbitraire, mais essentiellement différent de zéro; il vient ainsi

$$x_{\rho 6 + \alpha} = \varphi\left(x_{6 + \alpha},\ x_\alpha\right).$$

Cette équation exprime précisément la relation que nous nous proposions d'établir; elle montre très-facilement comment toutes les racines s'expriment de proche en proche, au moyen des deux racines arbitraires x_α, $x_{\alpha + 6}$, et met immédiatement en évidence dans quel ordre elles naissent ainsi les unes des autres.

Il est aisé de démontrer que, réciproquement, la relation précédente admise entre trois racines x_α, $x_{\alpha + 6}$, $x_{\alpha + \rho 6}$, entraîne la résolution par radicaux de l'équation.

A cet effet, soient θ une racine de l'équation binôme $x^n = 1$, et

$$F(\theta) = (x_0 + \theta x_1 + \theta^2 x^2 + \ldots + \theta^{n-1} x_{n-1})^n$$

la fonction résolvante de Lagrange. D'après la propriété caractéristique de cette fonction, on pourra, sans altérer sa valeur, ajouter aux indices des racines un nombre entier arbitraire α, et écrire

$$F(\theta) = (x_\alpha + \theta x_{\alpha+1} + \theta^2 x_{\alpha+2} + \ldots + \theta^{n-1} x_{\alpha+n-1})^n.$$

Cela posé, soit β un autre nombre entier arbitraire, mais différent de zéro et prenons β_0, de manière qu'on ait

$$\beta\beta_0 \equiv 1 \pmod{n};$$

on voit immédiatement que l'on a

$$F(\theta^{\beta_0}) = (x_\alpha + \theta x_{\alpha+\beta} + \theta^2 x_{\alpha+2\beta} + \ldots + \theta^{n-1} x_{\alpha+(n-1)\beta})^n,$$

et il est clair qu'en employant la relation

$$x_{\rho\beta+\alpha} = \varphi(x_{\beta+\alpha}, x_\alpha),$$

on pourra, par des substitutions successives, transformer le second membre en une fonction rationnelle Π des deux racines x_α, $x_{\alpha+\beta}$, de manière à avoir

$$F(\theta^{\beta_0}) = \Pi(x_\alpha, x_{\alpha+\beta})$$

pour une valeur quelconque de l'indice arbitraire α.

Cela étant, soit, comme plus haut, λ une racine de l'équation binôme $x^{n-1} = 1$, la fonction

$$\left[\begin{array}{l}\Pi(x_\alpha, x_{\alpha+\beta}) + \lambda\Pi(x_\alpha, x_{\alpha+\rho\beta}) + \lambda^2\Pi(x_\alpha, x_{\alpha+\rho^2\beta}) + \ldots \\ \qquad + \lambda^{n-2}\Pi(x_\alpha, x_{\alpha+\rho^{n-2}\beta})\end{array}\right]^{n-1}$$

conserve la même valeur quand on met $\rho\beta$ au lieu de β, c'est-à-dire qu'elle est indépendante de la valeur attribuée à β. Chacun des termes dont elle se compose est d'ailleurs indépendant de α;

donc, en la transformant au moyen de la relation

$$x_{\alpha+\rho\epsilon} = \varphi(x_{\alpha+\epsilon}, x_\alpha),$$

en une fonction rationnelle des deux seules racines x_α et $x_{\alpha+\epsilon}$, cette fonction devra se réduire à une quantité connue. Effectivement, si une fonction

$$u = \psi(x_{\alpha+\epsilon}, x_\alpha)$$

conserve la même valeur, quels que soient les indices α et ϵ, le second étant différent de zéro, on peut écrire

$$n(n-1)u = \sum_0^{n-1}{}_\alpha \sum_1^{n-1}{}_\epsilon \psi(x_{\alpha+\epsilon}, x_\alpha),$$

relation dont le second membre est une fonction symétrique de toutes les racines $x_0, x_1, \ldots, x_{n-1}$.

Il résulte de là que nous pouvons regarder les $n-1$ quantités

$$\Pi(x_\alpha, x_{\alpha+\epsilon}), \; \Pi(x_\alpha, x_{\alpha+\rho\epsilon}), \ldots, \; \Pi(x_\alpha, x_{\alpha+\rho^{n-2}\epsilon}),$$

comme les racines d'une équation abélienne résoluble par l'extraction d'un seul radical de degré $n-1$. Or ces quantités une fois obtenues, nous connaissons, pour toutes les valeurs de ϵ, excepté $\epsilon = 0$, la puissance $n^{ième}$ de la fonction résolvante $F(\theta^{\epsilon_0})$; donc, par l'extraction de $n-1$ radicaux du $n^{ième}$ degré, nous aurons ces diverses fonctions résolvantes, et, par conséquent, les racines elles-mêmes. On sait d'ailleurs, par une observation d'Abel, que ces $n-1$ radicaux s'expriment rationnellement en fonction de l'un d'entre eux et des quantités sur lesquelles ils portent, quantités qui sont, comme nous venons de le dire, les racines d'une équation abélienne.

NOTE XIV.

SUR L'ÉVALUATION APPROCHÉE DU PRODUIT $1.2.3\ldots x$, QUAND x EST UN GRAND NOMBRE.

La formule qui fait connaître la valeur approchée du produit $1.2.3\ldots x$ quand x est un grand nombre, est nécessaire pour l'intelligence de l'analyse que nous développerons dans la Note suivante. Je me propose ici d'établir le plus brièvement possible cette formule remarquable. Les méthodes les plus simples qui aient été proposées pour cet objet sont, à mon avis, celles que MM. Binet et Cauchy ont publiées dans ces dernières années (*). La marche que nous adoptons ne diffère pas essentiellement de celle qui a été suivie par M. Cauchy.

De la fonction $\Gamma(x)$.

Legendre a représenté par la notation $\Gamma(x)$ l'intégrale définie

$$\int_0^\infty \alpha^{x-1} e^{-\alpha}\, d\alpha,$$

où e désigne la base des logarithmes népériens. Cette fonction $\Gamma(x)$ constitue la seconde espèce des intégrales dites *eulériennes*; elle a une valeur finie pour toute valeur positive de x, mais elle est infinie lorsque x est nulle ou négative : nous supposerons toujours x réelle et positive (**).

En intégrant par parties la différentielle $\alpha^x e^{-\alpha}\, d\alpha$, il vient

$$\int \alpha^x e^{-\alpha}\, d\alpha = -\alpha^x e^{-\alpha} + x\int \alpha^{x-1} e^{-\alpha}\, d\alpha;$$

(*) *Voir* le XXVIII[e] cahier du *Journal de l'École Polytechnique*, et le tome II des *Exercices d'Analyse et de Physique mathématique* de M. Cauchy.

(**) Nous nous bornons ici aux seules propriétés des fonctions Γ qui sont nécessaires pour l'objet que nous avons en vue.

si l'on prend les intégrales entre les limites o et ∞, et si l'on observe que $\alpha^x e^{-\alpha}$ est nulle aux limites, il vient

$$\int_0^\infty \alpha^x e^{-\alpha} d\alpha = x \int_0^\infty \alpha^{x-1} e^{-\alpha} d\alpha,$$

c'est-à-dire

$$\Gamma(x+1) = x\Gamma(x).$$

Or on a évidemment

$$\Gamma(1) = \int_0^\infty e^{-\alpha} d\alpha = 1;$$

donc, dans le cas particulier de x entier, on a

$$\Gamma(x+1) = 1.2.3\ldots x.$$

Nous avons besoin encore, pour notre objet, de connaître la valeur de $\Gamma(x)$ pour $x = \frac{1}{2}$; le moyen le plus aisé d'obtenir cette valeur a été donné par Poisson dans son *Traité de Mécanique*. Voici en quoi il consiste. On a

$$\Gamma\left(\frac{1}{2}\right) = \int_0^\infty \alpha^{-\frac{1}{2}} e^{-\alpha} d\alpha,$$

ou, en posant $\alpha = x^2$,

$$\Gamma\left(\frac{1}{2}\right) = 2\int_0^\infty e^{-x^2} dx,$$

ou

$$\Gamma\left(\frac{1}{2}\right) = \int_{-\infty}^{+\infty} e^{-x^2} dx.$$

On aura aussi, en mettant y au lieu de x,

$$\Gamma\left(\frac{1}{2}\right) = \int_{-\infty}^{+\infty} e^{-y^2} dy,$$

et, par suite,

$$\Gamma^2\left(\frac{1}{2}\right) = \int_{-\infty}^{+\infty} e^{-x^2}\,dx \times \int_{-\infty}^{+\infty} e^{-y^2}\,dy$$
$$= \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} e^{-x^2-y^2}\,dx\,dy.$$

Si l'on pose

$$z = e^{-x^2-y^2},$$

et que l'on considère x, y, z comme des coordonnées rectangulaires, l'équation précédente représentera une surface S, et il est évident que l'expression $\Gamma^2\left(\frac{1}{2}\right)$ exprimera le volume indéfini compris entre le plan xy et la surface S. Cette surface est de révolution autour de l'axe des z, et la courbe méridienne a pour équation $z = e^{-x^2}$ dans le plan xz; cette considération va nous donner la valeur du volume représenté par $\Gamma^2\left(\frac{1}{2}\right)$. Décomposons ce volume en tranches parallèles au plan xy, et désignons par x l'abscisse de la courbe méridienne; l'expression des tranches dont il s'agit sera $\pi x^2\,dz$ et nous aurons à intégrer cette différentielle entre les limites $x = \infty$ et $x = 0$. Or on a

$$dz = -2x\,e^{-x^2}\,dx;$$

donc

$$\Gamma^2\left(\frac{1}{2}\right) = 2\pi\int_0^\infty x^3 e^{-x^2}\,dx,$$

ou, en posant $x = \alpha^{\frac{1}{2}}$,

$$\Gamma^2\left(\frac{1}{2}\right) = \pi\int_0^\infty \alpha\,e^{-\alpha}\,d\alpha = \pi\,\Gamma(2) = \pi;$$

extrayant la racine carrée, il vient

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}.$$

De la fonction $\log \Gamma(x)$.

Si, dans l'intégrale

$$(1) \qquad \Gamma(x) = \int_0^\infty \alpha^{x-1} e^{-\alpha}\, d\alpha,$$

on met $m\alpha$ au lieu de α, m étant une quantité positive, il vient

$$(2) \qquad \Gamma(x) = m^x \int_0^\infty \alpha^{x-1} e^{-m\alpha}\, d\alpha,$$

d'où

$$\frac{1}{m^x} = \frac{1}{\Gamma(x)} \int_0^\infty \alpha^{x-1} e^{-m\alpha}\, d\alpha,$$

formule dont on fait un fréquent usage. En particulier, pour $x = 1$, on a

$$(3) \qquad \frac{1}{m} = \int_0^\infty e^{-m\alpha}\, d\alpha;$$

multipliant cette équation par dm et intégrant ensuite entre les limites 1 et m, on obtient

$$(4) \qquad \log m = \int_0^\infty \frac{e^{-\alpha} - e^{-m\alpha}}{\alpha}\, d\alpha,$$

la caractéristique log désignant ici, comme dans tout ce qui va suivre, un logarithme népérien.

Si l'on fait successivement, dans l'équation (4), $m = 1, 2, 3, \ldots, (x-1)$ et qu'on ajoute ensuite tous les résultats, il viendra

$$\log 1.2\ldots(x-1) = \int_0^\infty \left[(x-1)e^{-\alpha} - \left(e^{-\alpha} + e^{-2\alpha} + \ldots + e^{-(x-1)\alpha}\right)\right]\frac{d\alpha}{\alpha},$$

ou, à cause de $1, 2 \ldots (x-1) = \Gamma(x)$,

$$(5) \quad \log \Gamma(x) = \int_0^\infty \left[(x-1)e^{-\alpha} - \frac{e^{-\alpha} - e^{-x\alpha}}{1 - e^{-\alpha}}\right]\frac{d\alpha}{\alpha}.$$

Cette formule (5) que nous venons d'obtenir, dans l'hypothèse de x entier, est générale et a lieu, quel que soit x.

En effet, la dérivée $\Gamma'(x)$ de $\Gamma(x)$ a pour valeur

$$\Gamma'(x) = \int_0^\infty \alpha^{x-1} e^{-\alpha} \log \alpha \, d\alpha;$$

or, par la formule (4), on a

$$\log \alpha = \int_0^\infty \frac{e^{-6} - e^{-\alpha 6}}{6} d6;$$

donc

$$\Gamma'(x) = \int_0^\infty \int_0^\infty \alpha^{x-1} e^{-\alpha} \left(e^{-6} - e^{-\alpha 6}\right) \frac{d\alpha}{6}$$

$$= \int_0^\infty \frac{d6}{6}\left[e^{-6}\int_0^\infty \alpha^{x-1} e^{-\alpha} d\alpha - \int_0^\infty \alpha^{x-1} e^{-(1+6)\alpha} d\alpha\right];$$

les intégrales relatives à α qui figurent dans cette valeur de $\Gamma'(x)$ ont respectivement pour valeurs $\Gamma(x)$ et $\frac{\Gamma(x)}{(1+6)^x}$, d'après les formules (1) et (2); donc on a

$$\Gamma'(x) = \Gamma(x) \int_0^\infty \left[e^{-6} - \frac{1}{(1+6)^x}\right] \frac{d6}{6}.$$

Divisant enfin par $\Gamma(x)$, de part et d'autre, il vient

$$\frac{d \log \Gamma(x)}{dx} = \int_0^\infty \left[e^{-6} - (1+6)^{-x}\right] \frac{d6}{6}.$$

Si l'on intègre, par rapport à x et à partir de $x = 1$, il vient, à cause de $\log \Gamma(1) = \log 1 = 0$,

$$(6) \quad \log \Gamma(x) = \int_0^\infty \left[(x-1)e^{-6} - \frac{(1+6)^{-1} - (1+6)^{-x}}{\log(1+6)}\right] \frac{d6}{6}.$$

A cause de $\log \Gamma(2) = 0$, on a, pour $x = 2$,

$$(7) \qquad 0 = \int_0^\infty \left[\frac{e^{-6}}{6} - \frac{(1+6)^{-2}}{\log(1+6)}\right] d6.$$

Ajoutons membre à membre les égalités (6) et (7), après avoir multiplié la seconde par $-(x-1)$, on aura cette nouvelle expression de $\log\Gamma(x)$, savoir :

$$(8)\ \log\Gamma(x)=\int_0^\infty\left[(x-1)(1+6)^{-2}-\frac{(1+6)^{-1}-(1+6)^{-x}}{6}\right]\frac{d6}{\log(1+6)}.$$

Enfin, si l'on pose

$$\log(1+6)=z,\quad \text{d'où}\quad 6=e^z-1,$$

il vient

$$(9)\qquad \log\Gamma(x)=\int_0^\infty\left[(x-1)e^{-z}-\frac{e^{-z}-e^{-xz}}{1-e^{-z}}\right]\frac{dz}{z},$$

ce qui n'est autre chose que la formule (5).

Détermination de la valeur approchée de $\log\Gamma(x)$, *quand* x *est un grand nombre.*

Nous poserons, avec M. Cauchy, les deux formules

$$(1)\qquad F(x)=\int_0^\infty\left[\left(x-1-\frac{1}{1-e^{-z}}\right)e^{-z}+\left(\frac{1}{z}+\frac{1}{2}\right)e^{-xz}\right]\frac{dz}{z},$$

$$(2)\qquad \varpi(x)=\int_0^\infty\left(\frac{1}{1-e^{-z}}-\frac{1}{z}-\frac{1}{2}\right)e^{-xz}\frac{dz}{z},$$

dont la seconde a été employée par M. Binet ; la valeur que nous avons trouvée pour $\log\Gamma(x)$ devient alors

$$(3)\qquad \log\Gamma(x)=F(x)+\varpi(x).$$

Il est aisé de calculer les valeurs des fonctions $F(x)$ et $\varpi(x)$ pour $x=\frac{1}{2}$. On a

$$\varpi\left(\frac{1}{2}\right)=\int_0^\infty\left(\frac{1}{1-e^{-z}}-\frac{1}{z}-\frac{1}{2}\right)e^{-\frac{1}{2}z}\frac{dz}{z},$$

ou, en remplaçant z par $2z$,

$$(4)\qquad \varpi\left(\frac{1}{2}\right) = \int_0^\infty \left(\frac{1}{1-e^{-2z}} - \frac{1}{2z} - \frac{1}{2}\right) e^{-z}\frac{dz}{z};$$

on a aussi

$$\begin{aligned}\varpi(1) &= \int_0^\infty \left(\frac{1}{1-e^{-z}} - \frac{1}{z} - \frac{1}{2}\right) e^{-z}\frac{dz}{z}\\ &= \int_0^\infty \left(\frac{1}{1-e^{-2z}} - \frac{1}{2z} - \frac{1}{2}\right) e^{-2z}\frac{dz}{z}.\end{aligned}$$

Égalant ces deux valeurs de $\varpi(1)$ et observant qu'on a identiquement

$$\frac{e^{-z}}{1-e^{-z}} - \frac{e^{-2z}}{1-e^{-2z}} = \frac{e^{-z}}{1-e^{-2z}},$$

il vient

$$(5)\qquad 0 = \int_0^\infty \left(\frac{1}{1-e^{-2z}} - \frac{2-e^{-z}}{2z} - \frac{1-e^{-z}}{2}\right) e^{-z}\frac{dz}{z};$$

en retranchant la formule (5) de la formule (4), il vient

$$\varpi\left(\frac{1}{2}\right) = \frac{1}{2}\int_0^\infty \left(\frac{e^{-z}-e^{-2z}}{z^2} - \frac{e^{-2z}}{z}\right) dz.$$

Or on a

$$\begin{aligned}\frac{1}{2}\left(\frac{e^{-z}-e^{-2z}}{z^2} - \frac{e^{-2z}}{z}\right) dz &= -\frac{1}{2} d\,\frac{e^{-z}-e^{-2z}}{z}\\ &\quad -\frac{1}{2}\,\frac{e^{-z}-e^{-2z}}{z}\,dz;\end{aligned}$$

intégrant de part et d'autre, entre les limites 0 et ∞, il vient

$$\varpi\left(\frac{1}{2}\right) = \frac{1}{2} - \frac{1}{2}\int_0^\infty \frac{e^{-z}-e^{-2z}}{z}\,dz,$$

et, à cause de la formule (4) du paragraphe précédent,

$$(6)\qquad \varpi\left(\frac{1}{2}\right) = \frac{1}{2} - \frac{1}{2}\log 2.$$

Maintenant, à cause de $\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}$, la formule (3) donne, en y faisant $x=\frac{1}{2}$,

$$(7) \qquad F\left(\frac{1}{2}\right)=\frac{1}{2}\log 2\pi-\frac{1}{2}.$$

Cela posé, on peut obtenir sous forme finie la valeur de $F(x)$, quelle que soit la variable x. En effet, si l'on différentie l'équation (1) par rapport à x, il vient

$$F'(x)=\int_0^\infty \frac{e^{-z}-e^{-xz}}{z}\,dz-\frac{1}{2}\int_0^\infty e^{-xz}\,dz,$$

et, en vertu des formules (3) et (4) du paragraphe précédent,

$$F'(x)=\log x-\frac{1}{2x};$$

intégrant et désignant par C une constante, il vient

$$F(x)=\left(x-\frac{1}{2}\right)\log x-x+C;$$

faisant $x=\frac{1}{2}$ et ayant égard à la formule (7), on trouve

$$C=\frac{1}{2}\log 2\pi,$$

et, par suite, on a

$$(8) \qquad F(x)=\left(x-\frac{1}{2}\right)\log x-x+\frac{1}{2}\log 2\pi;$$

la formule (3) devient alors

$$(9) \qquad \log\Gamma(x)=\left(x-\frac{1}{2}\right)\log x-x+\frac{1}{2}\log 2\pi+\varpi(x).$$

Il est aisé de trouver maintenant deux limites de la fonction $\varpi(x)$. A cet effet, posons

$$u=\frac{1}{1-e^{-z}}-\frac{1}{z}-\frac{1}{2},$$

on a

$$u = \frac{e^z(z-2)+z+2}{2z(e^z-1)}$$

$$= \frac{\frac{z^3}{1.2.3} + \frac{2z^4}{1.2.3.4} + \ldots + \frac{(n-2)z^n}{1.2\ldots n} + \ldots}{2z(e^z-1)};$$

on trouve aussi

$$\frac{z}{12} - u = \frac{e^z(z^2-6z+12) - z^2 - 6z - 12}{12z(e^z-1)}$$

$$= \frac{\frac{1.2}{1.2\ldots5}z^5 + \frac{2.3}{1.2\ldots6}z^6 + \ldots + \frac{(n-4)(n-3)}{1.2\ldots n}z^n + \ldots}{12z(e^z-1)}.$$

On conclut de là que, pour toute valeur positive de z, u est positif et moindre que $\frac{z}{12}$; il s'ensuit que l'on a

$$\varpi(x) > 0$$

et

$$\varpi(x) < \frac{1}{12}\int_0^\infty e^{-xz}\,dz < \frac{1}{12x}.$$

La formule (9) donne alors

$$(10)\quad \begin{cases} \log\Gamma(x) > \left(x-\frac{1}{2}\right)\log x - x + \frac{1}{2}\log 2\pi, \\ \log\Gamma(x) < \left(x-\frac{1}{2}\right)\log x - x + \frac{1}{2}\log 2\pi + \frac{1}{12x}. \end{cases}$$

On a ainsi deux limites de la fonction $\log\Gamma(x)$. En ajoutant $\log x$ aux deux membres de chacune de ces inégalités et se rappelant que $x\Gamma(x) = \Gamma(x+1)$, il vient

$$(11)\quad \begin{cases} \log\Gamma(x+1) > \left(x+\frac{1}{2}\right)\log x - x + \frac{1}{2}\log 2\pi, \\ \log\Gamma(x+1) < \left(x+\frac{1}{2}\right)\log x - x + \frac{1}{2}\log 2\pi + \frac{1}{12x}, \end{cases}$$

et, en revenant des logarithmes aux nombres,

$$(12)\qquad \begin{cases} \Gamma(x+1) > \sqrt{2\pi}\, e^{-x}\, x^{x+\frac{1}{2}}, \\ \Gamma(x+1) < \sqrt{2\pi}\, e^{-x}\, x^{x+\frac{1}{2}}\, e^{\frac{1}{12x}}. \end{cases}$$

On peut donc écrire, quel que soit x,

$$(13)\qquad \Gamma(x+1) = \sqrt{2\pi}\, e^{-x} x^{x+\frac{1}{2}}(1+\varepsilon),$$

et, dans le cas de x entier,

$$(14)\qquad 1.2.3\ldots x = \sqrt{2\pi}\, e^{-x}\, x^{x+\frac{1}{2}}(1+\varepsilon),$$

ε étant une quantité qui s'annule pour $x = \infty$.

Détermination de deux limites entre lesquelles reste comprise la somme des logarithmes népériens de tous les entiers qui ne surpassent pas un nombre donné.

Nous allons déduire de ce qui précède deux inégalités sur lesquelles nous aurons occasion de nous appuyer dans la Note suivante. Soit a un nombre entier, faisons $x = a+1$ dans la première des inégalités (10) du précédent paragraphe et $x = a$ dans la seconde des inégalités (11); on aura

$$(1)\qquad \begin{cases} \log 1.2.3\ldots a > \log\sqrt{2\pi} + (a+1)\log(a+1) - (a+1) - \frac{1}{2}\log(a+1), \\ \log 1.2.3\ldots a < \log\sqrt{2\pi} + a\log a - a + \frac{1}{2}\log a + \frac{1}{12a}. \end{cases}$$

Cela posé, désignons par x une quantité positive quelconque au moins égale à 1, et soit a le plus grand entier contenu dans x. On a, par hypothèse,

$$a \leqq x > a+1 \quad \text{et} \quad a \geqq 1;$$

on en déduit

$$\left(a+1-\frac{1}{2}\right)\left[\log(a+1)-1\right] > \left(x-\frac{1}{2}\right)(\log x - 1),$$

$$\left(a+\frac{1}{2}\right)(\log a - 1) + \frac{1}{12a} \overset{=}{<} \left(x+\frac{1}{2}\right)(\log x - 1) + \frac{1}{12},$$

ou

$$(2) \quad \begin{cases} (a+1)\log(a+1) - (a+1) - \frac{1}{2}\log(a+1) \\ > x\log x - x - \frac{1}{2}\log x, \\ a\log a - a + \frac{1}{2}\log a + \frac{1}{12a} \\ \overset{=}{<} x\log x - x + \frac{1}{2}\log x + \frac{1}{12}. \end{cases}$$

Des inégalités (1) et (2) on déduit, en appelant $T(x)$ le logarithme du produit de tous les nombres entiers qui ne surpassent pas x,

$$(3) \quad \begin{cases} T(x) > \log\sqrt{2\pi} + x\log x - x - \frac{1}{2}\log x, \\ T(x) < \log\sqrt{2\pi} + x\log x - x + \frac{1}{2}\log x + \frac{1}{12}. \end{cases}$$

Ces inégalités (3) sont celles que nous voulions obtenir.

NOTE XV.

SUR LA TOTALITÉ DES NOMBRES PREMIERS COMPRIS ENTRE DEUX LIMITES DONNÉES ET SUR LE POSTULATUM ADMIS DANS LA VINGTIÈME LEÇON.

Le problème qui consiste à déterminer combien il y a de nombres premiers compris entre deux nombres donnés n'a pas encore été résolu et semble présenter les plus grandes difficultés. M. Tchebichef est le premier qui se soit occupé avec succès de cette question; dans un Mémoire présenté en 1850 à l'Académie impériale des Sciences de Saint-Pétersbourg, cet habile géomètre a donné le moyen d'assigner deux limites entre lesquelles est nécessairement compris le nombre qui exprime combien il y a de nombres premiers entre deux nombres donnés. M. Tchebichef a déduit de son analyse la démonstration rigoureuse du postulatum de M. Bertrand, postulatum qui consiste, comme on sait, en ce que :

Il y a toujours au moins un nombre premier compris entre a et $2a - 2$ si a est supérieur à $\frac{7}{2}$.

Bien que je sois parvenu à démontrer le théorème de M. Bertrand sans avoir recours à son postulatum (Note VIII), je ne crois pas inutile de présenter ici l'analyse ingénieuse par laquelle M. Tchebichef a obtenu la démonstration de ce postulatum, et qui repose sur des considérations entièrement neuves.

Nous désignerons par $T(z)$, comme nous l'avons déjà fait dans la Note précédente, la somme des logarithmes népériens de tous les nombres entiers qui ne surpassent pas z; nous désignerons en outre par $\theta(z)$ la somme des logarithmes népériens de tous les nombres *premiers* qui ne surpassent pas z. Les fonctions $T(z)$ et $\theta(z)$ se réduisent à zéro lorsque z est inférieur

à 2. Quand z sera une quantité composée, comme $\left(\frac{x}{2}\right)^{\frac{1}{2}}$ par exemple, nous écrirons, pour abréger, $\theta\left(\frac{x}{2}\right)^{\frac{1}{2}}$ au lieu de $\theta\left[\left(\frac{x}{2}\right)^{\frac{1}{2}}\right]$.

Propriété fondamentale de la fonction $\theta(z)$.

La propriété fondamentale sur laquelle reposent les recherches de M. Tchebichef, consiste dans l'égalité suivante :

$$
\begin{aligned}
T(x) = {} & \theta(x) + \theta(x)^{\frac{1}{2}} + \theta(x)^{\frac{1}{3}} + \theta(x)^{\frac{1}{4}} + \ldots \\
& + \theta\left(\frac{x}{2}\right) + \theta\left(\frac{x}{2}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{4}} + \ldots \\
& + \theta\left(\frac{x}{3}\right) + \theta\left(\frac{x}{3}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{4}} + \ldots \\
& + \theta\left(\frac{x}{4}\right) + \theta\left(\frac{x}{4}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{4}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{4}\right)^{\frac{1}{4}} + \ldots \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

où les séries doivent être prolongées jusqu'aux termes qui deviennent zéro (*).

Pour démontrer cette égalité, remarquons que chaque membre est égal à une somme de termes tels que $k \log \alpha$, k désignant un entier et α un nombre premier. Supposons que dans la suite des nombres 1, 2, 3, 4, ..., qui ne surpassent pas x,

(*) M. A. de Polignac, dans des recherches intéressantes sur les nombres premiers, a obtenu, de son côté, cette relation remarquable. Un extrait du Mémoire de M. de Polignac a été publié dans les *Comptes rendus de l'Académie des Sciences*, avant que le travail de M. Tchebichef fût connu en France.

il y en ait A_1 qui soient divisibles par α; nommons aussi A_2 le nombre de ceux qui sont divisibles par α^2, et généralement A_i le nombre de ceux qui sont divisibles par α^i; il est clair que le coefficient de log α dans $T(x)$ sera $A_1 + A_2 + A_3 + \ldots$. Considérons maintenant les termes qui composent une ligne verticale du second membre de notre égalité, par exemple,

$$\theta(x)^{\frac{1}{i}}, \quad \theta\left(\frac{x}{2}\right)^{\frac{1}{i}}, \quad \theta\left(\frac{x}{3}\right)^{\frac{1}{i}}, \quad \theta\left(\frac{x}{4}\right)^{\frac{1}{i}}, \ldots:$$

on trouvera, dans cette suite, autant de termes contenant log α avec le coefficient 1, qu'il y a de quantités qui ne sont pas inférieures à α dans la suite

$$x^{\frac{1}{i}}, \quad \left(\frac{x}{2}\right)^{\frac{1}{i}}, \quad \left(\frac{x}{3}\right)^{\frac{1}{i}}, \quad \left(\frac{x}{4}\right)^{\frac{1}{i}}, \ldots.$$

Or le nombre de ces quantités est évidemment le même que le nombre des quantités

$$\alpha^i, \quad 2\alpha^i, \quad 3\alpha^i, \quad 4\alpha^i, \quad \ldots,$$

qui ne surpassent pas x; ce nombre est précisément celui que nous avons désigné par A_i. Donc le coefficient de log α dans le deuxième membre de notre égalité est $A_1 + A_2 + A_3 + \ldots$, ce qui démontre l'exactitude de cette égalité.

Nous ferons, pour abréger

$$(1) \qquad \psi(z) = \theta(z) + \theta(z)^{\frac{1}{2}} + \theta(z)^{\frac{1}{3}} + \theta(z)^{\frac{1}{4}} + \ldots,$$

et alors l'égalité que nous venons d'établir pourra s'écrire ainsi :

$$(2) \quad T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \ldots.$$

Démonstration de deux inégalités auxquelles satisfait la fonction $\psi(z)$.

Les deux inégalités que nous nous proposons d'établir sont

les suivantes :

$$\psi(x) > T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right),$$

$$\psi(x) - \psi\left(\frac{x}{6}\right) < T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right).$$

L'équation (2) donne

$$(3)\quad \left\{\begin{array}{l} T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \ldots \\ + \psi\left(\frac{x}{30}\right) + \psi\left(\frac{x}{2.30}\right) + \psi\left(\frac{x}{3.30}\right) + \psi\left(\frac{x}{4.30}\right) + \ldots \\ - \psi\left(\frac{x}{2}\right) - \psi\left(\frac{x}{2.2}\right) - \psi\left(\frac{x}{3.2}\right) - \psi\left(\frac{x}{4.2}\right) - \ldots \\ - \psi\left(\frac{x}{3}\right) - \psi\left(\frac{x}{2.3}\right) - \psi\left(\frac{x}{3.3}\right) - \psi\left(\frac{x}{4.3}\right) - \ldots \\ - \psi\left(\frac{x}{5}\right) - \psi\left(\frac{x}{2.5}\right) - \psi\left(\frac{x}{3.5}\right) - \psi\left(\frac{x}{4.5}\right) - \ldots . \end{array}\right.$$

Le second membre de cette équation est de la forme

$$A_1\psi(x) + A_2\psi\left(\frac{x}{2}\right) + A_3\psi\left(\frac{x}{3}\right) + \ldots + A_n\psi\left(\frac{x}{n}\right) + \ldots,$$

A_1, A_2, A_3, etc., étant des coefficients entiers. Or je dis qu'on a en général,

$A_n = 1$, si n n'est divisible par aucun des facteurs 2, 3, 5;

$A_n = 0$, si n est divisible par un seul des facteurs 2, 3, 5;

$A_n = -1$, si n est divisible par deux des facteurs 2, 3, 5;

$A_n = -1$, si n est divisible par les facteurs 2, 3, 5, c'est-à-dire par 30.

En effet, dans le premier cas, où n n'est divisible par aucun des nombres 2, 3, 5, on ne trouve le terme $\psi\left(\frac{x}{n}\right)$ que dans

la première ligne horizontale du second membre de l'équation (3). Dans le second cas, où n est divisible par un seul des nombres 2, 3, 5, on trouvera le terme $\psi\left(\frac{x}{n}\right)$ avec le signe — dans l'une des trois dernières lignes horizontales du second membre de l'équation (3), et comme ce terme existe dans la première ligne avec le signe +, on trouvera zéro, après la réduction, pour coefficient de $\psi\left(\frac{x}{n}\right)$. Dans le troisième cas, où n est divisible par deux des nombres 2, 3, 5, le terme $\psi\left(\frac{x}{n}\right)$ se trouve avec le signe + dans la première ligne horizontale du second membre de l'équation (3), et avec le signe — dans deux des trois dernières lignes; donc il ne restera après la réduction que $-\psi\left(\frac{x}{n}\right)$. Enfin dans le quatrième cas, où n est divisible par chacun des nombres 2, 3, 5, le terme $\psi\left(\frac{x}{n}\right)$ se trouve avec le signe + dans les deux premières lignes du second nombre de l'équation (3), et avec le signe — dans les trois dernières lignes; il restera donc encore $-\psi\left(\frac{x}{n}\right)$ après la réduction. Donc, pour

$$\begin{array}{rllllllllll} n = 30m + & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, \\ & 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18, & 19, & 20, \\ & 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28, & 29, & 30, \end{array}$$

on a

$$\begin{array}{rllllllllll} A_n = & 1, & 0, & 0, & 0, & 0, & -1, & 1, & 0, & 0, & -1, \\ & 1, & -1, & 1, & 0, & -1, & 0, & 1, & -1, & 1, & -1, \\ & 0, & 0, & 1, & -1, & 0, & 0, & 0, & 0, & 1, & -1, \end{array}$$

et, par conséquent, l'équation (3) se réduit à

$$T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)$$
$$=\psi(x)-\psi\left(\frac{x}{6}\right)+\psi\left(\frac{x}{7}\right)-\psi\left(\frac{x}{10}\right)+\psi\left(\frac{x}{11}\right)-\psi\left(\frac{x}{12}\right)+\ldots,$$

où tous les termes du second membre ont pour coefficient $+1$ et -1 alternativement. Or la fonction $\psi(z)$ ne peut croître quand z décroît; donc la série

$$\psi(x)-\psi\left(\frac{x}{6}\right)+\psi\left(\frac{x}{7}\right)-\psi\left(\frac{x}{10}\right)+\ldots,$$

qui forme le second membre de l'équation précédente, est comprise entre

$$\psi(x) \quad \text{et} \quad \psi(x)-\psi\left(\frac{x}{6}\right);$$

on a donc

$$(4)\quad \begin{cases} \psi(x) \geqq T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right), \\ \psi(x)-\psi\left(\frac{x}{6}\right) \leqq T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right); \end{cases}$$

ce qu'il fallait démontrer.

Détermination de deux limites entre lesquelles sont comprises les fonctions $\psi(z)$ et $\theta(z)$.

On a vu, dans la Note précédente, que la fonction $T(x)$ satisfait aux deux inégalités

$$(5)\quad \begin{cases} T(x) < \log\sqrt{2\pi}+x\log x - x+\frac{1}{2}\log x+\frac{1}{12}, \\ T(x) > \log\sqrt{2\pi}+x\log x - x-\frac{1}{2}\log x. \end{cases}$$

On déduit de là

$$T(x) + T\left(\frac{x}{30}\right) < 2\log\sqrt{2\pi}$$

$$+\frac{2}{12} + \frac{31}{30}x\log x - x\log 30^{\frac{1}{30}} - \frac{31}{30}x + \log x - \frac{1}{2}\log 30,$$

$$T(x) + T\left(\frac{x}{30}\right) > 2\log\sqrt{2\pi}$$

$$+\frac{31}{30}x\log x - x\log 30^{\frac{1}{30}} - \frac{31}{30}x - \log x + \frac{1}{2}\log 30,$$

et

$$T\left(\frac{x}{2}\right) + T\left(\frac{x}{3}\right) + T\left(\frac{x}{5}\right) < 3\log\sqrt{2\pi} + \frac{3}{12}$$

$$+\frac{31}{30}x\log x - x\log 2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}} - \frac{31}{30}x + \frac{3}{2}\log x - \frac{1}{2}\log 30,$$

$$T\left(\frac{x}{2}\right) + T\left(\frac{x}{3}\right) + T\left(\frac{x}{5}\right) > 3\log\sqrt{2\pi}$$

$$+\frac{31}{30}x\log x - x\log 2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}} - \frac{31}{30}x - \frac{3}{2}\log x + \frac{1}{2}\log 30.$$

Retranchant la quatrième de ces inégalités de la première, et la troisième de la seconde, il vient

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

$$< x\log\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}}{30^{\frac{1}{30}}} + \frac{5}{2}\log x - \frac{1}{2}\log 1800\pi + \frac{2}{12},$$

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

$$> x\log\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}}{30^{\frac{1}{30}}} - \frac{5}{2}\log x + \frac{1}{2}\log\frac{450}{\pi} - \frac{3}{12}.$$

Nous ferons, pour abréger,

$$A = \log\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}}{30^{\frac{1}{30}}} = 0,92129202\ldots,$$

et alors les inégalités précédentes deviennent

$$(6)\quad \begin{cases} T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right) \\ \qquad < Ax+\frac{5}{2}\log x-\frac{1}{2}\log 1800\pi+\frac{2}{12}, \\ T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right) \\ \qquad > Ax-\frac{5}{2}\log x+\frac{1}{2}\log\frac{450}{\pi}-\frac{3}{12}, \end{cases}$$

et l'on voit que l'on a, à fortiori,

$$(7)\quad \begin{cases} T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)<Ax+\frac{5}{2}\log x, \\ T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)>Ax-\frac{5}{2}\log x-1. \end{cases}$$

Les formules (5) n'ont lieu que dans l'hypothèse de $x>1$; d'ailleurs, pour former les inégalités (6), on a remplacé dans (5) x par $\frac{x}{2}$, $\frac{x}{3}$, $\frac{x}{5}$, $\frac{x}{30}$; donc les formules (6) ne sont établies que dans l'hypothèse de $x>30$. Mais il est aisé de vérifier que les formules (7) ont lieu pour toutes les valeurs de x comprises entre 1 et 30, et, par suite, qu'elles ne présentent aucune exception.

Des inégalités (4) et (7) on déduit

$$(8)\quad \begin{cases} \psi(x)>Ax-\frac{5}{2}\log x-1, \\ \psi(x)-\psi\left(\frac{x}{6}\right)<Ax+\frac{5}{2}\log x. \end{cases}$$

La première de ces inégalités donne immédiatement une limite inférieure de $\psi(x)$; la seconde peut servir, comme on va voir, à obtenir une limite supérieure. Pour cela, posons

$$f(x)=\frac{6}{5}Ax+\frac{5}{4\log 6}\log^2 x+\frac{5}{4}\log x,$$

on aura

$$f\left(\frac{x}{6}\right)=\frac{1}{5}\,\mathrm{A}x+\frac{5}{4\log 6}\log^2 x-\frac{5}{4}\log x,$$

et, par suite,

$$f(x)-f\left(\frac{x}{6}\right)=\mathrm{A}x+\frac{5}{2}\log x;$$

on a donc

$$\psi(x)-\psi\left(\frac{x}{6}\right)<f(x)-f\left(\frac{x}{6}\right),$$

ou bien

$$\psi(x)-f(x)<\psi\left(\frac{x}{6}\right)-f\left(\frac{x}{6}\right);$$

en changeant successivement x en $\frac{x}{6}, \frac{x}{6^2}, \frac{x}{6^3}, \ldots, \frac{x}{6^{m+1}}$, il vient

$$(9)\begin{cases}\psi(x)-f(x)<\psi\left(\frac{x}{6}\right)-f\left(\frac{x}{6}\right)<\psi\left(\frac{x}{6^2}\right)-f\left(\frac{x}{6^2}\right)<\ldots\\ \quad<\psi\left(\frac{x}{6^{m+1}}\right)-f\left(\frac{x}{6^{m+1}}\right).\end{cases}$$

Supposons maintenant que m soit le plus grand entier qui vérifie la condition $6^m \overset{=}{<} x$; $\frac{x}{6^{m+1}}$ tombera entre 1 et $\frac{1}{6}$ et, par suite, $\psi\left(\frac{x}{6^{m+1}}\right)$ sera nul; je dis de plus que $-f\left(\frac{x}{6^{m+1}}\right)$ sera plus petit que 1. En effet, la valeur de $-f(z)$ peut s'écrire ainsi,

$$-f(z)=\frac{5\log 6}{16}-\frac{5}{4\log 6}\left(\log z+\frac{1}{2}\log 6\right)^2-\frac{6}{5}\mathrm{A}z;$$

d'où l'on conclut

$$-f(z)<\frac{5\log 6}{16},$$

et, à fortiori,

$$-f(z) < 1,$$

puisque 6 étant moindre que e^3, log 6 est inférieur à 3.

D'après cela, la formule (9) donne

$$\psi(x) - f(x) < 1,$$

et, par suite,

$$(10)\quad \psi(x) < \frac{6}{5}Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x + 1.$$

Les deux limites que nous venons de trouver pour la fonction $\psi(x)$ vont nous permettre de trouver également deux limites de la fonction $\theta(x)$.

Pour cela remarquons que la formule

$$\psi(z) = \theta(z) + \theta(z)^{\frac{1}{2}} + \theta(z)^{\frac{1}{3}} + \ldots$$

donne

$$\psi(x) - \psi(\sqrt{x}) = \theta(x) + \theta(x)^{\frac{1}{3}} + \theta(x)^{\frac{1}{5}} + \theta(x)^{\frac{1}{7}} + \ldots,$$

$$\psi(x) - 2\psi(\sqrt{x}) = \theta(x) - \left[\theta(x)^{\frac{1}{2}} - \theta(x)^{\frac{1}{3}}\right] - \left[\theta(x)^{\frac{1}{4}} - \theta(x)^{\frac{1}{5}}\right] - \ldots$$

Or la fonction $\theta(z)$ est positive ou nulle, et d'ailleurs elle ne peut croître quand z décroît; donc on a

$$(11)\quad \begin{cases} \theta(x) \leqq \psi(x) - \psi(\sqrt{x}), \\ \theta(x) \geqq \psi(x) - 2\psi(\sqrt{x}). \end{cases}$$

Mais on vient de trouver

$$(12)\quad \begin{cases} \psi(x) < \frac{6}{5}Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x + 1, \\ \psi(x) > Ax - \frac{5}{2}\log x - 1, \end{cases}$$

et l'on en tire

$$(13)\quad \begin{cases} \psi(\sqrt{x}) < \frac{6}{5}\mathrm{A}x^{\frac{1}{2}} + \frac{5}{16\log 6}\log^2 x + \frac{5}{8}\log x + 1, \\ \psi(\sqrt{x}) > \mathrm{A}x^{\frac{1}{2}} - \frac{5}{4}\log x - 1; \end{cases}$$

ce qui donne, en vertu des inégalités (11),

$$(14)\quad \begin{cases} \theta(x) < \frac{6}{5}\mathrm{A}x - \mathrm{A}x^{\frac{1}{2}} + \frac{5}{4\log 6}\log^2 x + \frac{5}{2}\log x + 2, \\ \theta(x) > \mathrm{A}x - \frac{12}{5}\mathrm{A}x^{\frac{1}{2}} - \frac{5}{8\log 6}\log^2 x - \frac{15}{4}\log x - 3. \end{cases}$$

Ainsi, la somme des logarithmes de tous les nombres premiers qui ne surpassent pas x est comprise entre les limites

$$\frac{6}{5}\mathrm{A}x - \mathrm{A}x^{\frac{1}{2}} + \frac{5}{4\log 6}\log^2 x + \frac{5}{2}\log x + 2,$$
$$\mathrm{A}x - \frac{12}{5}\mathrm{A}x^{\frac{1}{2}} - \frac{5}{8\log 6}\log^2 x - \frac{15}{4}\log x - 3.$$

Détermination de deux limites du nombre qui indique combien il y a de nombres premiers compris entre deux nombres donnés.

Soit m le nombre qui indique combien il y a de nombres premiers plus grands qu'un nombre donné l et qui ne surpassent pas un autre nombre donné L. La somme des logarithmes népériens de ces m nombres premiers, sera évidemment comprise entre $m\log l$ et $m\log \mathrm{L}$; on aura donc

$$\theta(\mathrm{L}) - \theta(l) > m\log l,$$
$$\theta(\mathrm{L}) - \theta(l) < m\log \mathrm{L},$$

et, par conséquent,

$$m < \frac{\theta(\mathrm{L}) - \theta(l)}{\log l}, \quad m > \frac{\theta(\mathrm{L}) - \theta(l)}{\log \mathrm{L}};$$

mais, d'après les inégalités (14), on a

$$\theta(\mathrm{L}) - \theta(l) < \mathrm{A}\left(\frac{6}{5}\mathrm{L} - l\right) - \mathrm{A}\left(\mathrm{L}^{\frac{1}{2}} - \frac{12}{5}l^{\frac{1}{2}}\right)$$
$$+ \frac{5}{8\log 6}(2\log^2\mathrm{L} + \log^2 l) + \frac{5}{4}(2\log\mathrm{L} + 3\log l) + 5,$$
$$\theta(\mathrm{L}) - \theta(l) > \mathrm{A}\left(\mathrm{L} - \frac{6}{5}l\right) - \mathrm{A}\left(\frac{12}{5}\mathrm{L}^{\frac{1}{2}} - l^{\frac{1}{2}}\right)$$
$$- \frac{5}{8\log 6}(\log^2\mathrm{L} + 2\log^2 l) - \frac{5}{4}(3\log\mathrm{L} + 2\log l) - 5;$$

donc

$$(15)\ \begin{cases} m < \dfrac{\mathrm{A}\left(\frac{6}{5}\mathrm{L} - l\right) - \mathrm{A}\left(\mathrm{L}^{\frac{1}{2}} - \frac{12}{5}l^{\frac{1}{2}}\right) + \frac{5}{8\log 6}(2\log^2\mathrm{L} + \log^2 l) + \frac{5}{4}(2\log\mathrm{L} + 3\log l) + 5}{\log l}, \\ m > \dfrac{\mathrm{A}\left(\mathrm{L} - \frac{6}{5}l\right) - \mathrm{A}\left(\frac{12}{5}\mathrm{L}^{\frac{1}{2}} - l^{\frac{1}{2}}\right) - \frac{5}{8\log 6}(\log^2\mathrm{L} + 2\log^2 l) - \frac{5}{4}(3\log\mathrm{L} + 2\log l) - 5}{\log\mathrm{L}}. \end{cases}$$

Ces formules (15) donnent ainsi deux limites entre lesquelles tombe la quantité m qui désigne combien il y a de nombres premiers plus grands que l et qui ne surpassent pas L. La deuxième de ces formules montre qu'on trouvera plus de k nombres premiers entre les limites l et L, si la condition suivante est satisfaite, savoir :

$$(16)\ k < \frac{\mathrm{A}\left(\mathrm{L} - \frac{6}{5}l\right) - \mathrm{A}\left(\frac{12}{5}\mathrm{L}^{\frac{1}{2}} - l^{\frac{1}{2}}\right) - \frac{5}{8\log 6}(\log^2\mathrm{L} + 2\log^2 l) - \frac{5}{4}(3\log\mathrm{L} + 2\log l) - 5}{\log\mathrm{L}},$$

et comme l est > 0 et $< \mathrm{L}$, on vérifie cette inégalité (16) en faisant

$$k = \frac{\mathrm{A}\left(\mathrm{L} - \frac{6}{5}l\right) - \frac{12}{5}\mathrm{A}\mathrm{L}^{\frac{1}{2}} - \frac{15}{8\log 6}\log^2\mathrm{L} - \frac{25}{4}\log\mathrm{L} - 5}{\log\mathrm{L}},$$

d'où l'on tire

$$l = \frac{5}{6}\mathrm{L} - 2\mathrm{L}^{\frac{1}{2}} - \frac{25}{16\,\mathrm{A}\log 6}\log^2\mathrm{L} - \frac{5}{6\mathrm{A}}\left(\frac{25}{4} + k\right)\log\mathrm{L} - \frac{25}{6\mathrm{A}}.$$

Ainsi, en prenant pour l cette valeur, on est sûr de trouver plus

de k nombres premiers entre l et L. Il est bien entendu que l et L sont supposés plus grands que 1.

En faisant $k = 0$, on peut conclure de ce qui précède qu'il y a au moins un nombre premier entre l et L, si l'on prend

$$(18)\quad l = \frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25\log^2 L}{16\,A\log 6} - \frac{125\log L}{24\,A} - \frac{25}{6A}.$$

Démonstration du postulatum de M. Bertrand.

Des résultats que nous venons d'obtenir, il est aisé de déduire la démonstration du postulatum de M. Bertrand. Effectivement, nous venons de voir qu'il y a au moins un nombre premier entre les limites

$$\frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25\log^2 L}{16\,A\log 6} - \frac{125\log L}{24\,A} - \frac{25}{6A} \quad \text{et} \quad L;$$

donc il sera établi qu'il y a au moins un nombre premier entre les limites a et $2a - 2$, si l'on prouve qu'on peut, par une valeur convenable de L, satisfaire aux deux inégalités

$$2a - 2 > L,$$

$$a < \frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25\log^2 L}{16\,A\log 6} - \frac{125\log L}{24\,A} - \frac{25}{6A}.$$

Or, on vérifie évidemment la première de ces inégalités en prenant

$$L = 2a - 3.$$

Quant à la seconde, elle devient pour $L = 2a - 3$,

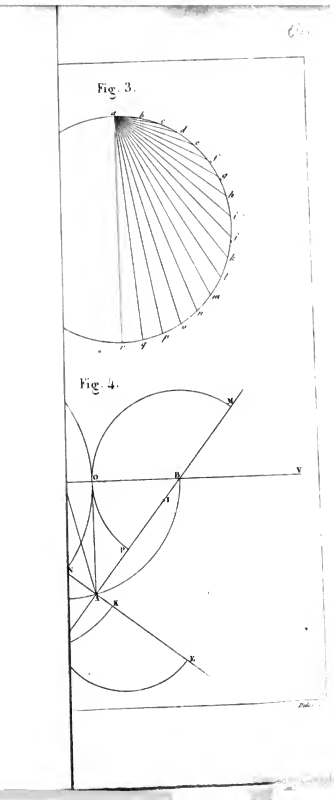
$$a < \frac{5}{6}(2a-3) - 2\sqrt{2a-3} - \frac{25\log^2(2a-3)}{16\,A\log 6}$$
$$- \frac{125\log(2a-3)}{24\,A} - \frac{25}{6A},$$

ce qui est exact pour toutes les valeurs de a qui surpassent la plus grande racine de l'équation

$$(19)\quad \begin{cases} x = \frac{5}{6}(2x-3) - 2\sqrt{2x-3} - \frac{25\log^2(2x-3)}{16\,A\log 6} \\ \quad - \frac{125\log(2x-3)}{24\,A} - \frac{25}{6\,A}; \end{cases}$$

or on trouve que cette plus grande racine est comprise entre 159 et 160; donc si a est > 160, il y a nécessairement un nombre premier compris entre a et $2a-2$. A l'égard des valeurs de a inférieures à 160, le postulatum de M. Bertrand peut se vérifier immédiatement au moyen des Tables de nombres premiers.

FIN DES NOTES.


Fig. 3.
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
Fig. 4.
M
O
B
V
I
P
N
A
K
E

